CLAIMS

1. An information sending system for sending predetermined contents data from an information sending apparatus to an information receiving apparatus, wherein said information sending apparatus comprises:

means for holding identification information to identify said information sending apparatus encrypted by a distribution key unique to said information receiving apparatus;

means for adding said identification information to said contents data in order to make a comparison with said identification information encrypted by said distribution key; and

means for sending said identification information encrypted by said distribution key together with said contents data with said identification information added; and

said information receiving apparatus comprises:

means for holding said distribution key;

means for receiving said contents data with said identification information added and said identification information encrypted by said distribution key;

means for decrypting by said distribution key said identification information encrypted by the distribution key; and

means for comparing said identification information added to said contents data with said decrypted identification information.

2. The information sending system according to claim 1, wherein said information sending apparatus comprises:

means for generating handling policies, that is, generating contents handling policies prescribing conditions for using said contents data and storing said identification information, and

said means for adding identification information adds said contents handling policies to said contents data.

3. The information sending system according to claim 1, wherein said means for adding identification information of said information sending apparatus directly adds said identification information to said contents data.

4. The information sending system according to claim 1, wherein said information sending apparatus comprises:

means for encrypting said contents data by a predetermined content key;

means for encrypting said contents key by a predetermined individual key;

means for adding signature data for checking illegal data and tampering to said contents key encrypted by said individual key and said identification information encrypted by said distribution key; and

said information receiving apparatus comprises means for verifying said signature data.

5. The information sending system according to claim 4, wherein said means for adding a signature of said information sending apparatus adds said signature data to said contents data encrypted by said content key, and if album contents data storing a plurality of said contents data encrypted by said content key to which the signature data is added is generated, it also adds said signature data to the album contents data; and

said means for verifying a signature of said information receiving apparatus verifies said signature data added to said album contents data, and if it determines that said album contents data is correct data as a result of the verification, it omits verification of said signature data added to each of said contents data encrypted by said content key stored in said album contents data.

6. The information sending system according to claim 5, wherein said means for adding a signature of said information sending apparatus adds said signature data to said contents key encrypted by said individual key and said identification information encrypted by said distribution key respectively, and corresponding to said album contents data, if album key data is generated by storing a plurality of said contents keys encrypted by said individual key and said identification information encrypted by said distribution key to which said signature data is added, it also adds said signature data to the album key data; and

said means for verifying a signature of said information receiving apparatus verifies said signature data added to said album key data, and if it determines that said album key data is correct data as a result of the verification, it omits verification of said signature data added to said contents key encrypted by said individual key and said identification information encrypted by said distribution key stored in the album key data respectively.

7. The information sending system according to claim 6, wherein said information sending apparatus comprises:

means for generating handling policies, that is, generating contents handling policies prescribing conditions for using said contents data and storing said identification information, and

said means for adding a signature of said information sending apparatus adds said signature data to said contents data handling policies, and corresponding to said album contents data, if album handling policies are generated by storing a plurality of said contents handling policies to which said signature data is added, it also adds said signature data to the album handling policies; and

said means for verifying a signature of said information receiving apparatus verifies said signature data added to said album handling policies, and if it determines that said album handling policies are correct data as a result of the verification, it omits verification of said signature data added to said contents handling policies stored in the album handling policies.

8. The information sending system according to claim 7, wherein said information sending apparatus comprises the means for:

creating contents price information showing a price for said contents data, and

said means for adding a signature of said information sending apparatus adds said signature data to said contents price information, and corresponding to said album contents data, if album price information data storing a plurality of said contents price information to which said signature data is added is generated, it also adds said signature data to the album price information; and

said means for verifying a signature of said information receiving apparatus verifies said signature data added to said album price information, and if it determines that said album price information is correct data as a result of the verification, it omits verification of said signature data added to said contents price information stored in the album price information.

9. The information sending system according to claim 8 wherein:

said means for generating handling policies of said information sending apparatus generates said contents handling policies storing signature verification information representing whether or not said signature data added to said contents data encrypted by said content key is verified; and

said means for verifying a signature of said information receiving apparatus verifies said signature data added to said contents data encrypted by said content key only when instructed to verify said signature data added to said contents data encrypted by said content key based on said signature verification information stored in said contents handling policies.

10. The information sending system according to claim 9 wherein:

said means for generating handling policies of said information sending apparatus generates said contents handling policies storing said signature verification information representing whether or not said signature data added to said album contents data is verified; and

said means for verifying a signature of said information receiving apparatus verifies said signature data added to said album contents data only when instructed to verify said signature data added to the album contents data based on said signature verification information stored in said contents handling policies.

11. The information sending system according to claim 8 wherein:

said means for creating price information of said information sending apparatus creates said contents price information storing signature verification information representing whether or not said signature data added to said contents data encrypted by said content key is verified; and

said means for verifying a signature of said information receiving apparatus verifies said signature data added to said contents data encrypted by said content key only when instructed to verify said signature data added to said contents data encrypted by the content key based on said signature verification information stored in said contents price information.

12. The information sending system according to claim 11 wherein:

said means for creating price information of said information sending apparatus creates said contents price information storing said signature verification information representing whether or not said signature data added to said album contents data is verified; and

said means for verifying a signature of said information receiving apparatus verifies said signature data added to said album contents data only when instructed to verify said signature data added to the album contents data based on said signature verification information stored in said contents price information.

13. The information sending system according to claim 12 wherein:

said means for generating handling policies of said information sending apparatus generates said contents handling policies prescribing that another specific contents data of said may be acquired only when said specific contents data is acquired.

14. An information sending apparatus for sending predetermined contents data to an information receiving apparatus, comprising:

means for holding identification information to identify said information sending apparatus encrypted by a distribution key unique to said information receiving apparatus;

means for adding said identification information to said contents data in order to make a comparison with said identification information encrypted by said distribution key; and

means for sending said identification information encrypted by said distribution key together with said contents data with said identification information added.

15. The information sending apparatus according to claim 14 comprising:

means for generating handling policies, that is, generating contents handling policies prescribing conditions for using said contents data and storing said identification information, and wherein:

said means for adding identification information adds said contents handling policies to said contents data.

16. The information sending apparatus according to claim 14 wherein:

said means for adding identification information adds said identification information to said contents data.

17. The information sending apparatus according to claim 14, comprising:

means for encrypting said contents data by a predetermined content key;

means for encrypting said contents key by a predetermined individual key;

means for adding signature data for checking illegal data and tampering to said contents key encrypted by said individual key and said identification information encrypted by said distribution key in said information receiving apparatus.

18. The information sending apparatus according to claim 17, wherein said means for adding a signature adds said signature data to said contents data encrypted by said content key, and if album contents data storing a plurality of said contents data encrypted by said content key to which said signature data is added is generated, it also adds said signature data to the album contents data.

19. The information sending apparatus according to claim 18, wherein said means for adding a signature adds said signature data to said contents key encrypted by said individual key and said identification information encrypted by said distribution key respectively, and corresponding to said album contents data, if album key data is generated by storing a plurality of the contents keys encrypted by said individual key and said identification information encrypted by said distribution

key to which said signature data is added, it also adds said signature data to the album key data.

20. The information sending apparatus according to claim 19, comprising the means for generating handling policies, that is, generating contents handling policies prescribing conditions for using said contents data and storing said identification information, and wherein:

said means for adding a signature adds said signature data to said contents data handling policies, and corresponding to said album contents data, if album handling policies are generated by storing a plurality of said contents handling policies to which said signature data is added, it also adds said signature data to the album handling policies.

21. The information sending apparatus according to claim 20, comprising the means for creating contents price information showing a price for said contents data, and wherein:

said means for adding a signature adds said signature data to said contents price information, and corresponding to said album contents data, if album price information data storing a plurality of said contents price information to which said signature data is added is generated, it also adds said signature data to the album price information.

22. The information sending apparatus according to claim 21 wherein:

said means for generating handling policies generates said contents handling policies storing signature verification information representing whether or not said signature data added to said contents data encrypted by said content key is verified

23. The information sending apparatus according to claim 22 wherein:

said means for generating handling policies generates said contents handling policies storing said signature verification information representing whether or not said signature data added to said album contents data is verified.

24. The information sending apparatus according to claim 21 wherein:

said means for creating price information creates said contents price information storing signature verification information representing whether or not said signature data added to said contents data encrypted by said content key is verified.

25. The information sending apparatus according to claim 24 wherein:

said means for creating price information creates said contents price information storing said signature verification information representing whether or not said signature data added to said album contents data is verified.

26. The information sending apparatus according to claim 25 wherein:

said means for generating handling policies generates said contents handling policies prescribing that another specific contents data of said may be acquired only when said specific contents data is acquired.

27. An information receiving apparatus for receiving predetermined contents data sent from an information sending apparatus, comprising:

means for holding a predetermined distribution key unique to said information receiving apparatus;

means for receiving said contents data with identification information added to identify said information sending apparatus and said identification information encrypted by said distribution key sent from said information sending apparatus;

means for decrypting by said distribution key said identification information encrypted by the distribution key; and

means for comparing said identification information added to said contents data with said decrypted identification information.

28. The information receiving apparatus according to claim 27, comprising:

means for performing a purchasing procedure for said contents data; and wherein:

said means for receiving receives said contents data sent from said information sending apparatus and contents handling policies

prescribing conditions for using said contents data added to the contents data and storing said identification information;

said means for comparing compares said identification information stored in said contents handling policies with said identification information that is decrypted; and

when said identification information compared in said means for comparing mutually matches, said means for performing a purchasing procedure performs said purchasing procedure of said contents data by using said contents handling policies.

29. The information receiving apparatus according to claim 27, wherein:

said means for receiving receives said contents data sent from said information sending apparatus and said identification information directly added to the contents data.

30. The information receiving apparatus according to claim 27, comprising the means for verifying a signature, that is, verifying signature data added to said content key encrypted by said individual key and said identification information encrypted said distribution key sent from said information sending apparatus together with said contents data encrypted by a predetermined contents key and said contents key encrypted by a predetermined individual key, and detecting whether or not said content key encrypted by said individual key and

said identification information encrypted said distribution key are illegal data and tampered data.

31. The information receiving apparatus according to claim 30, wherein said means for verifying a signature verifies said signature data added to said album contents data, of said signature data added to said contents data encrypted by said content key and said signature data added to album contents data storing a plurality of said contents data encrypted by said content key, sent from said information sending apparatus, and if it determines that said album contents data is correct data as a result of the verification, it omits verification of said signature data added to each of said contents data encrypted by said content key stored in the album contents data.

32. The information receiving apparatus according to claim 31, wherein said means for verifying a signature verifies said signature data added to the album key data, of said signature data added said contents key encrypted by said individual key and said identification information encrypted by said distribution key respectively and said signature data added to album key data storing a plurality of said contents keys encrypted by said individual key and said identification information encrypted by said distribution key to which said signature data is added corresponding to said album contents data, sent from said information sending apparatus, and if it determines that said album key data is correct data as a result of the verification, it omits verification

of said signature data added to said contents key encrypted by said individual key and said identification information encrypted by said distribution key stored in the album key data respectively.

33. The information receiving apparatus according to claim 32, wherein said means for verifying a signature verifies said signature data added to album handling policies, of said signature data added to contents handling policies prescribing conditions for using said contents data and storing said identification information and said signature data added to said album handling policies storing a plurality of said contents handling policies to which said signature data is added corresponding to said album contents data, sent from said information sending apparatus, and if it determines that said album handling policies are correct data as a result of the verification, it omits verification of said signature data added to said contents handling policies stored in the album handling policies.

34. The information receiving apparatus according to claim 33, wherein said means for verifying a signature verifies said signature data added to the album price information, of said signature data added to contents price information showing a price for said contents data and said signature data added to the album price information data storing a plurality of said contents price information to which said signature data is added corresponding to said album contents data, sent from said information sending apparatus, and if it determines that said album

price information is correct data as a result of the verification, it omits verification of said signature data added to said contents price information stored in the album price information.

35. The information receiving apparatus according to claim 34, wherein said means for verifying a signature verifies said signature data added to said contents data encrypted by said content key, only when instructed to verify said signature data based on said signature verification information stored in the contents handling policies, of said contents data encrypted by said content key, said signature data added to said contents data encrypted by said content key and said contents handling policies storing signature verification information representing whether or not the signature data is verified, sent from said information sending apparatus.

36. The information receiving apparatus according to claim 35, wherein said means for verifying a signature verifies said signature data added to said album contents data, only when instructed to verify said signature data based on said signature verification information stored in the contents handling policies, of said album contents data, said signature data added to said album contents data and said contents handling policies storing said signature verification information representing whether or not the signature data is verified, sent from said information sending apparatus.

37. The information receiving apparatus according to claim 34, wherein said means for verifying a signature verifies said signature data added to said contents data encrypted by said content key, only when instructed to verify said signature data based on said signature verification information stored in the contents price information, of said contents data encrypted by said content key, said signature data added to said contents data encrypted by the content key, and said contents price information storing signature verification information representing whether or not the signature data is verified, sent from said information sending apparatus.

38. The information receiving apparatus according to claim 37, wherein said means for verifying a signature verifies said signature data added to said album contents data, only when instructed to verify said signature data based on said signature verification information stored in the contents price information, of said album contents data, said signature data added to the album contents data and said contents price information storing said signature verification information representing whether or not the signature data is verified, sent from said information sending apparatus.

39. The information receiving apparatus according to claim 38, wherein said means for receiving receives said contents handling policies prescribing that receipt of another specific contents data of said is allowed only when said specific contents data is acquired.

40. An information sending method for sending predetermined contents data from an information sending apparatus to an information receiving apparatus, comprising:

an identification information adding step of, by said information sending apparatus, adding to said contents data identification information to identify the information sending apparatus; and

a sending step of, by said information sending apparatus, sending contents data with said identification information added and identification information to identify said information sending apparatus encrypted by a distribution key unique to said information receiving apparatus;

a receiving step of, by said information receiving apparatus, receiving said contents data with said identification information added and said identification information encrypted by said distribution key;

a decrypting step of, in said information receiving apparatus, decrypting by said distribution key said identification information encrypted by said distribution key; and

a comparing step of, by said information receiving apparatus, comparing said identification information added to said contents data with said decrypted identification information.

41. The information sending method according to claim 40, comprising:

a handling policies generating step of, by said information sending apparatus, generating contents handling policies prescribing

conditions for using said contents data and storing said identification information, and

a handling policies adding step of adding said contents handling policies to said contents data.

42. The information sending method according to claim 40, wherein said identification information adding step directly adds said identification information to said contents data.

43. The information sending method according to claim 40, comprising:

a contents data encrypting step of, by said information sending apparatus, encrypting said contents data by a predetermined content key;

a contents key encrypting step of, by said information sending apparatus, encrypting said contents key by a predetermined individual key;

a signature adding step of, by said information sending apparatus, adding signature data for checking illegal data and tampering to said contents key encrypted by said individual key and said identification information encrypted by said distribution key; and

a signature verifying step of, by said information receiving apparatus, verifying said signature data added to said contents key encrypted by individual key and identification information encrypted by said distribution key.

44. The information sending method according to claim 43, wherein said signature adding step adds said signature data to said contents data encrypted by said content key, and if album contents data storing a plurality of said contents data encrypted by said content key to which the signature data is added is generated, it also adds said signature data to the album contents data; and

said signature verifying step verifies said signature data added to said album contents data, and if it determines that said album contents data is correct data as a result of the verification, it omits verification of said signature data added to each of said contents data encrypted by said content key stored in said album contents data.

45. The information sending method according to claim 44, wherein said signature adding step adds said signature data to said contents key encrypted by said individual key and said identification information encrypted by said distribution key respectively, and corresponding to said album contents data, if album key data is generated by storing a plurality of contents key encrypted by said individual key and said identification information encrypted by said distribution key to which said signature data is added, it also adds said signature data to the album key data; and

said signature verifying step verifies said signature data added to said album key data, and if it determines that said album key data is correct data as a result of the verification, it omits verification of said signature data added to said contents key encrypted by said

individual key and said identification information encrypted by said distribution key stored in said album key data respectively.

46. The information sending method according to claim 45, comprising a handling policies generating step of generating contents handling policies prescribing conditions for using said contents data and storing said identification information, and wherein:

said signature adding step adds said signature data to said contents data handling policies, and corresponding to said album contents data, if album handling policies are generated by storing a plurality of said contents handling policies to which said signature data is added, it also adds said signature data to the album handling policies; and

said signature verifying step verifies said signature data added to said album handling policies, and if it determines that said album handling policies are correct data as a result of the verification, it omits verification of said signature data added to said contents handling policies stored in the album handling policies.

47. The information sending method according to claim 46, comprising the step of creating contents price information showing a price for said contents data, and wherein:

said signature adding step adds said signature data to said contents price information, and corresponding to said album contents data, if album price information data storing a plurality of said

contents price information to which said signature data is added is generated, it also adds said signature data to the album price information; and

said signature verifying step verifies said signature data added to said album price information, and if it determines that said album price information is correct data as a result of the verification, it omits verification of said signature data added to said contents price information stored in the album price information.

48. The information sending method according to claim 47 wherein:

said handling policies generating step generates said contents handling policies storing signature verification information representing whether or not said signature data added to said contents data encrypted by said content key is verified; and

said signature verifying step verifies said signature data added to said contents data encrypted by said content key only when instructed to verify said signature data added to said contents data encrypted by the content key based on said signature verification information stored in said contents handling policies.

49. The information sending method according to claim 48 wherein:

said handling policies generating step generates said contents handling policies storing said signature verification information representing whether or not said signature data added to said album contents data is verified; and

said signature verifying step verifies said signature data added to said album contents data only when instructed to verify said signature data added to the album contents data based on said signature verification information stored in said contents handling policies.

50. The information sending method according to claim 47 wherein:

said price information creating step creates said contents price information storing signature verification information representing whether or not said signature data added to said contents data encrypted by said content key is verified; and

said signature verifying step verifies said signature data added to said contents data encrypted by said content key only when instructed to verify said signature data added to said contents data encrypted by said content key based on said signature verification information stored in said contents price information.

51. The information sending method according to claim 50 wherein:

said price information creating step creates said contents price information storing said signature verification information representing whether or not said signature data added to said album contents data is verified; and

said signature verifying step verifies said signature data added to said album contents data only when instructed to verify said signature data added to said album contents data based on said signature verification information stored in said contents price information.

52. The information sending method according to claim 51 wherein:

said handling policies generating step generates said contents handling policies prescribing that another specific contents data of said may be acquired only when said specific contents data is acquired.

53. An information sending method for sending predetermined contents data to an information receiving apparatus, comprising:

an identification information adding step of adding said identification information to said contents data in order to make a comparison with identification information for identifying said information sending apparatus encrypted by a predetermined distribution key unique to said information receiving apparatus and held in advance; and

a sending step of sending said identification information encrypted by said distribution key to said information receiving apparatus together with said contents data with said identification information added.

54. The information sending method according to claim 53 comprising the steps of:

a handling policies generating step of generating contents handling policies prescribing conditions for using said contents data and storing said identification information, and wherein:

a handling policies adding step of adding said contents handling policies to said contents data.

55. The information sending method according to claim 53 wherein:

said identification information adding step directly adds said identification information to said contents data.

56. The information sending method according to claim 53, comprising:

a contents data encrypting step of encrypting said contents data by a predetermined content key;

a contents key encrypting step of encrypting said contents key by a predetermined individual key;

a signature adding step of adding signature data for checking illegal data and tampering to said contents key encrypted by said individual key and said identification information encrypted by said distribution key in said information receiving apparatus.

57. The information sending method according to claim 56, wherein said signature adding step adds said signature data to said contents data encrypted by said content key, and if album contents data storing a plurality of said contents data encrypted by said content key to which said signature data is added is generated, it also adds said signature data to the album contents data.

58. The information sending method according to claim 57, wherein said signature adding step adds said signature data to said contents key encrypted by said individual key and said identification information encrypted by said distribution key respectively, and corresponding to said album contents data, if album key data is generated by storing a plurality of the contents keys encrypted by said individual key and said identification information encrypted by said distribution key to which said signature data is added, it also adds said signature data to the album key data.

59. The information sending method according to claim 58, comprising a handling policies generating step of generating contents handling policies prescribing conditions for using said contents data and storing said identification information, and wherein:

said signature adding step adds said signature data to said contents data handling policies, and corresponding to said album contents data, if album handling policies are generated by storing a plurality of said contents handling policies to which said signature data is added, it also adds said signature data to the album handling policies.

60. The information sending method according to claim 59, comprising a price information creating step of creating contents price information showing a price for said contents data, and wherein:

said signature adding step adds said signature data to said contents price information, and corresponding to said album contents data, if album price information data storing a plurality of said contents price information to which said signature data is added is generated, it also adds said signature data to the album price information.

61. The information sending method according to claim 60 wherein:

said handling policies generating step generates said contents handling policies storing signature verification information representing whether or not said signature data added to said contents data encrypted by said content key is verified.

62. The information sending method according to claim 61 wherein:

said handling policies generating step generates said contents handling policies storing said signature verification information representing whether or not said signature data added to said album contents data is verified.

63. The information sending method according to claim 60 wherein:

said price information creating step creates said contents price information storing signature verification information representing whether or not said signature data added to said contents data encrypted by said content key is verified.

64. The information sending method according to claim 63 wherein:

said price information creating step creates said contents price information storing said signature verification information representing whether or not said signature data added to said album contents data is verified.

65. The information sending method according to claim 64 wherein:

said handling policies generating step generates said contents handling policies prescribing that another specific contents data of said may be acquired only when said specific contents data is acquired.

66. An information receiving method for receiving predetermined contents data sent from an information sending apparatus, comprising:

a receiving step of receiving said contents data with identification information added to identify said information sending apparatus and said identification information encrypted by a predetermined distribution key unique to said information receiving apparatus sent from said information sending apparatus;

a decrypting step of decrypting by said distribution key said identification information encrypted by the distribution key; and

a comparing step of comparing said identification information added to said contents data with said decrypted identification information.

67. The information receiving method according to claim 66, comprising a purchasing step of performing a purchasing procedure for said contents data, wherein:

said receiving step receives said contents data sent from said information sending apparatus and contents handling policies prescribing conditions for using said contents data added to the contents data and storing said identification information;

said comparing step compares said identification information stored in said contents handling policies with said identification information that is decrypted; and

when said identification information compared in said comparing step mutually matches, said purchasing step performs said purchasing procedure of said contents data by using said contents handling policies.

68. The information receiving method according to claim 66, wherein:

said comparing step compares said identification information directly added to said contents data with said decrypted identification information.

69. The information receiving method according to claim 66, comprising a signature verifying step of verifying signature data added to said content key encrypted by said individual key and said identification information encrypted said distribution key sent from said information sending apparatus together with said contents data encrypted by the

predetermined content key and said contents key encrypted by the predetermined individual key, and detecting whether or not said content key encrypted by said individual key and said identification information encrypted said distribution key are illegal data and tampered data.

70. The information receiving method according to claim 69, wherein said signature verifying step verifies said signature data added to said album contents data, of said signature data added to said contents data encrypted by said content key and said signature data added to album contents data storing a plurality of said contents data encrypted by said content key, sent from said information sending apparatus, and if it determines that said album contents data is correct data as a result of the verification, it omits verification of said signature data added to each of said contents data encrypted by said content key stored in the album contents data.

71. The information receiving method according to claim 70, wherein said signature verifying step verifies said signature data added to the album key data, of said signature data added to said contents key encrypted by said individual key and said identification information encrypted by said distribution key respectively and said signature data added to album key data storing a plurality of said contents keys encrypted by said individual key and said identification information encrypted by said distribution key corresponding to said album contents

data, sent from said information sending apparatus, and if it determines that said album key data is correct data as a result of the verification, it omits verification of said signature data added to said contents key encrypted by said individual key and said identification information encrypted by said distribution key stored in the album key data respectively.

72. The information receiving method according to claim 71, wherein said signature verifying step verifies said signature data added to the album handling policies, of said signature data added to contents handling policies prescribing conditions for using said contents data and storing said identification information and said signature data added to said album handling policies storing a plurality of said contents handling policies corresponding to said album contents data, sent from said information sending apparatus, and if it determines that said album handling policies are correct data as a result of the verification, it omits verification of said signature data added to said contents handling policies stored in the album handling policies.

73. The information receiving method according to claim 72, wherein said signature verifying step verifies said signature data added to the album price information, of said signature data added to contents price information showing a price for said contents data and said signature data added to the album price information data storing a plurality of said contents price information corresponding to said

album contents data, sent from said information sending apparatus, and if it determines that said album price information is correct data as a result of the verification, it omits verification of said signature data added to said contents price information stored in the album price information.

74. The information receiving method according to claim 73, wherein said signature verifying step verifies said signature data added to said contents data encrypted by the content key, only when instructed to verify said signature data based on said signature verification information stored in the contents handling policies, of said contents data encrypted by said content key, said signature data added to said contents data encrypted by said content key and said contents handling policies storing signature verification information representing whether or not the signature data is verified, sent from said information sending apparatus.

75. The information receiving method according to claim 74, wherein said signature verifying step verifies said signature data added to said album contents data, only when instructed to verify said signature data based on said signature verification information stored in the contents handling policies, of said album contents data, said signature data added to said album contents data and said contents handling policies storing said signature verification information representing

whether or not the signature data is verified, sent from said information sending apparatus.

76. The information receiving method according to claim 73, wherein said signature verifying step verifies said signature data added to said contents data encrypted by said content key, only when instructed to verify said signature data based on said signature verification information stored in the contents price information, of said contents data encrypted by said content key, said signature data added to said contents data encrypted by the content key, and said contents price information storing signature verification information representing whether or not the signature data is verified, sent from said information sending apparatus.

77. The information receiving method according to claim 76, wherein said signature verifying step verifies said signature data added to said album contents data, only when instructed to verify said signature data based on said signature verification information stored in the contents price information, of said album contents data, said signature data added to the album contents data and said contents price information storing said signature verification information representing whether or not the signature data is verified, sent from said information sending apparatus.

78. The information receiving method according to claim 77 wherein:

said receiving step receives said contents handling policies prescribing that another specific contents data of said may be acquired only when said specific contents data is acquired.

79. A program storage medium storing a predetermined program and supplying the program to an information sending apparatus, characterized in that said program comprises:

an identification information adding step of adding said identification information to said contents data in order to make a comparison with identification information for identifying said information sending apparatus encrypted by a predetermined distribution key unique to said information receiving apparatus and held in advance; and

a sending step of sending to said information receiving apparatus said identification information encrypted by said distribution key together with said contents data with said identification information added.

80. The program storage medium according to claim 79, characterized in that said program comprises:

a handling policies generating step of generating contents handling policies prescribing conditions for using said contents data and storing said identification information; and

a handling policies adding step of adding said contents handling policies to said contents data.

81. The program storage medium according to claim 79 wherein:

said identification information adding step of said program adds said identification information to said contents data.

82. The program storage medium according to claim 79, characterized in that said program comprises:

a contents data encrypting step of encrypting said contents data by a predetermined content key;

a contents key encrypting step of encrypting said contents key by a predetermined individual key;

a signature adding step of adding signature data for checking illegal data and tampering to said contents key encrypted by said individual key and said identification information encrypted by said distribution key in said information receiving apparatus.

83. The program storage medium according to claim 82, wherein said signature adding step of said program adds said signature data to said contents data encrypted by said content key, and if album contents data storing a plurality of said contents data encrypted by said content key to which said signature data is added is generated, it also adds said signature data to the album contents data.

84. The program storage medium according to claim 83, wherein said signature adding step of said program adds said signature data to said

contents key encrypted by said individual key and said identification information encrypted by said distribution key respectively, and corresponding to said album contents data, if album key data is generated by storing a plurality of the contents keys encrypted by said individual key and said identification information encrypted by said distribution key to which said signature data is added, it also adds said signature data to the album key data.

85. The program storage medium according to claim 84, characterized in that said program comprises a handling policies generating step of generating contents handling policies prescribing conditions for using said contents data and storing said identification information, and wherein:

said signature adding step adds said signature data to said contents data handling policies, and corresponding to said album contents data, if album handling policies are generated by storing a plurality of said contents handling policies to which said signature data is added, it also adds said signature data to the album handling policies.

86. The program storage medium according to claim 85, characterized in that said program comprises a price information creating step of creating contents price information showing a price for said contents data, and wherein:

said signature adding step adds said signature data to said contents price information, and corresponding to said album contents data, if album price information data storing a plurality of said contents price information to which said signature data is added is generated, it also adds said signature data to the album price information.

87. The program storage medium according to claim 86 wherein:

said handling policies generating step of said program generates said contents handling policies storing signature verification information representing whether or not said signature data added to said contents data encrypted by said content key is verified.

88. The program storage medium according to claim 87 wherein:

said handling policies generating step of said program generates said contents handling policies storing said signature verification information representing whether or not said signature data added to said album contents data is verified.

89. The program storage medium according to claim 86 wherein:

said price information creating step of said program creates said contents price information storing signature verification information representing whether or not said signature data added to said contents data encrypted by said content key is verified.

90. The program storage medium according to claim 89 wherein:

said price information creating step of said program creates said contents price information storing said signature verification information representing whether or not said signature data added to said album contents data is verified.

91. The program storage medium according to claim 90 wherein:

said handling policies generating step of said program generates said contents handling policies prescribing that another specific contents data of said may be acquired only when said specific contents data is acquired.

92. A program storage medium for storing a predetermined program and supplying the program to an information receiving apparatus, characterized in that said program comprises:

a receiving step of receiving predetermined contents data with identification information added to identify said information sending apparatus and said identification information encrypted by a predetermined distribution key unique to the information receiving apparatus sent from said information sending apparatus;

a decrypting step of decrypting by said distribution key said identification information encrypted by the distribution key; and

a comparing step of comparing said identification information added to said contents data with said decrypted identification information.

93. The program storage medium according to claim 92, characterized in that said program comprises a purchasing step of performing a purchasing procedure for said contents data; and wherein:

said receiving step receives said contents data sent from said information sending apparatus and contents handling policies prescribing conditions for using said contents data added to the contents data and storing said identification information;

said comparing step compares said identification information stored in said contents handling policies with said identification information that is decrypted; and

when said identification information compared in said comparing step mutually matches, said purchasing step performs said purchasing procedure of said contents data by using said contents handling policies.

94. The program storage medium according to claim 92, wherein:

said comparing step of said program compares said identification information directly added to said contents data with said identification information that is decrypted.

95. The program storage medium according to claim 92, characterized in that said program comprises a signature verifying step of verifying signature data added to said content key encrypted by said individual key and said identification information encrypted said distribution

key sent from said information sending apparatus together with said contents data encrypted by a predetermined contents key and said contents key encrypted by a predetermined individual key, and detecting whether or not said content key encrypted by said individual key and said identification information encrypted said distribution key are illegal data and tampered data.

96. The program storage medium according to claim 95, wherein a signature verifying step of said program verifies said signature data added to the album contents data, of said signature data added to said contents data encrypted by said content key and said signature data added to album contents data storing a plurality of said contents data encrypted by said content key, sent from said information sending apparatus, and if it determines that said album contents data is correct data as a result of the verification, it omits verification of said signature data added to each of said contents data encrypted by said content key stored in the album contents data.

97. The program storage medium according to claim 96, wherein said signature verifying step of said program verifies said signature data added to the album key data, of said signature data added said contents key encrypted by said individual key and said identification information encrypted by said distribution key respectively and said signature data added to album key data storing a plurality of said contents keys encrypted by said individual key and said identification

information encrypted by said distribution key corresponding to said album contents data, sent from said information sending apparatus, and if it determines that said album key data is correct data as a result of the verification, it omits verification of said signature data added to said contents key encrypted by said individual key and said identification information encrypted by said distribution key stored in the album key data respectively.

98. The program storage medium according to claim 97, wherein said signature verifying step of said program verifies said signature data added to the album handling policies, of said signature data added to contents handling policies prescribing conditions for using said contents data and storing said identification information and said signature data added to said album handling policies storing a plurality of said contents handling policies corresponding to said album contents data, sent from said information sending apparatus, and if it determines that said album handling policies are correct data as a result of the verification, it omits verification of said signature data added to said contents handling policies stored in the album handling policies.

99. The program storage medium according to claim 98, wherein said signature verifying step of said program verifies said signature data added to the album price information, of said signature data added to contents price information showing a price for said contents data and said signature data added to the album price information data storing

a plurality of said contents price information corresponding to said album contents data, sent from said information sending apparatus, and if it determines that said album price information is correct data as a result of the verification, it omits verification of said signature data added to said contents price information stored in the album price information.

100. The program storage medium according to claim 99, wherein said signature verifying step of said program verifies said signature data added to said contents data encrypted by said content key, only when instructed to verify said signature data based on said signature verification information stored in the contents handling policies, of said contents data encrypted by said content key, said signature data added to said contents data encrypted by said content key and said contents handling policies storing signature verification information representing whether or not the signature data is verified, sent from said information sending apparatus.

101. The program storage medium according to claim 100, wherein said signature verifying step of said program verifies said signature data added to said album contents data, only when instructed to verify said signature data based on said signature verification information stored in the contents handling policies, of said album contents data, said signature data added to the album contents data and said contents handling policies storing said signature verification information

representing whether or not the signature data is verified, sent from said information sending apparatus.

102. The program storage medium according to claim 99, wherein said signature verifying step of said program verifies said signature data added to said contents data encrypted by the content key, only when instructed to verify said signature data based on said signature verification information stored in the contents price information, of said contents data encrypted by said content key, said signature data added to said contents data encrypted by the content key and said contents price information storing signature verification information representing whether or not the signature data is verified, sent from said information sending apparatus.

103. The program storage medium according to claim 102, wherein said signature verifying step of said program verifies said signature data added to the album contents data, only when instructed to verify said signature data based on said signature verification information stored in the contents price information, of said album contents data, said signature data added to the album contents data and said contents price information storing said signature verification information representing whether or not the signature data is verified, sent from said information sending apparatus.

104. The program storage medium according to claim 103, wherein said receiving step of said program receives said contents handling policies prescribing that receipt of another specific contents data of said is allowed only when said specific contents data is acquired.

105. An information sending system for sending predetermined contents data from an information sending apparatus to an information receiving apparatus, wherein:

said information sending apparatus comprises means for sending, together with said contents data, data of the maximum number of times of possible resending predefined to the contents data; and

said information receiving apparatus comprises:

means for receiving, together with said contents data, data of maximum number of times;

means for generating data of the remaining number of times of possible resending of said contents data based on said data of maximum number of times; and

means for resending, that is, sending data of the remaining number of times together with said contents data.

106. The information sending system according to claim 105, wherein:

said means for generating data of the number of times of said information receiving apparatus generates, based on a source of said contents data, a via-apparatus data showing an apparatus by way of which the contents data is sent; and

said means for resending sends said via-apparatus data together with said contents data and said data of the remaining number of times.

107. An information sending apparatus for sending predetermined contents data to an information receiving apparatus, comprising means for sending to said information receiving apparatus, together with said contents data, data of the maximum number of times of possible resending predefined to the contents data.

108. An information receiving apparatus for receiving predetermined contents data sent from an information sending apparatus, comprising:

means for receiving said contents data and data of the maximum number of times of possible resending predefined to the contents data, sent from said information sending apparatus; and

means for generating data of the remaining number of times of possible resending of said contents data based on said data of maximum number of times; and

means for resending, that is, sending data of the remaining number of times together with said contents data.

109. The information receiving apparatus according to claim 108, wherein:

said means for generating data of the number of times generates, based on a source of said contents data, a via-apparatus data showing an apparatus by way of which the contents data is sent; and

said means for resending sends said via-apparatus data together with said contents data and said data of the remaining number of times.

110. An information sending method for sending predetermined contents data from an information sending apparatus to an information receiving apparatus, comprising:

a sending step of sending by said information sending apparatus, together with said contents data, data of the maximum number of times of possible resending predefined to the contents data;

a receiving step of, by said information receiving apparatus, said data of maximum number of times together with said contents data;

a number of times data generating step of, by said information receiving apparatus, generating data of the remaining number of times of possible resending of said contents data based on said data of maximum number of times; and

a resending step of, by said information receiving apparatus, sending data of the remaining number of times together with said contents data.

111. The information sending method according to claim 110, wherein:

said number of times data generating step generates, based on a source of said contents data, a via-apparatus data showing an apparatus by way of which the contents data is sent; and

said resending step sends said via-apparatus data together with said contents data and said data of the remaining number of times.

112. An information sending method for sending predetermined contents data to an information receiving apparatus, comprising a sending step of sending to said information receiving apparatus, together with said contents data, data of the maximum number of times of possible resending predefined to the contents data.

113. An information receiving method for receiving predetermined contents data sent from an information sending apparatus, comprising:

a receiving step of receiving said contents data and data of the maximum number of times of possible resending predefined to the contents data sent from an information sending apparatus;

a number of times data generating step of generating data of the remaining number of times of possible resending of said contents data based on said data of maximum number of times; and

a resending step of sending data of said remaining number of times together with said contents data.

114. The information receiving method according to claim 113, wherein:

said means for generating data of the number of times generates, based on a source of said contents data, a via-apparatus data showing an apparatus by way of which the contents data is sent; and

said means for resending sends said via-apparatus data together with said contents data and said data of the remaining number of times.

115. A program storage medium storing a predetermined program and supplying the program to an information sending apparatus, characterized in that said program comprises:

a sending step of sending to the information receiving apparatus, together with predetermine contents data, data of the maximum number of times of possible resending predefined to the contents data.

116. A program storage medium storing a predetermined program and supplying the program to an information receiving apparatus, characterized in that said program comprises:

a receiving step of receiving predetermined contents data and data of the maximum number of times of possible resending predefined to the contents data sent from an information sending apparatus; and

a number of times data generating step of generating data of the remaining number of times of possible resending of said contents data based on said data of maximum number of times; and

a resending step of sending data of the remaining number of times together with said contents data.

117. The program storage medium according to claim 116, wherein:

said means for generating data of the number of times of said program generates, based on a source of said contents data, a via-apparatus data showing an apparatus by way of which the contents data is sent; and

said means for resending sends said via-apparatus data together with said contents data and said data of the remaining number of times.

118. A recording and reproducing system for recording and reproducing by a recording and reproducing apparatus predetermined contents data sent from an information sending apparatus on a removable data storage apparatus, wherein:

said information sending apparatus comprises:

means for encrypting said contents data by a predetermined content key; and

means for sending said content key and said contents data encrypted by the content key; and

said recording and reproducing apparatus comprises:

means for receiving said content key and said contents data encrypted by the content key sent from said information sending apparatus;

means for controlling recording and reproducing for sending out the received content key and said contents data encrypted by the content key to said data storage apparatus and having them recorded thereby or having said content key and said contents data encrypted by the content key reproduced from said data storage apparatus to read them; and

said data storage apparatus comprises:

a predetermined record medium;

means for holding a predetermined save key;

means for encrypting a content key by said save key;

means for recording and reproducing, that is, recording said content key encrypted by said save key and said contents data encrypted by the content key on said record medium or reproducing said content key encrypted by said save key and said contents data encrypted by the content key from the record medium; and means for decrypting by said save key said content key encrypted by the save key.

119. The recording and reproducing system according to claim 118, wherein said means for holding a save key is tamper resistant in said data storage apparatus.

120. The recording and reproducing system according to claim 119, wherein said means for controlling recording and reproducing limits said data storage apparatus as to reproduction of said contents data encrypted by said content key recorded on said record medium.

121. The recording and reproducing system according to claim 120, wherein said limitation of reproduction is the number of times of possible reproduction of said contents data.

122. The recording and reproducing system according to claim 120, wherein said limitation of reproduction is the period of possible reproduction of said contents data.

123. The recording and reproducing system according to claim 118, wherein said recording and reproducing apparatus comprises means for decrypting contents, that is, decrypting by using said content key said contents data encrypted by the content key read from said data storage apparatus.

124. The recording and reproducing system according to claim 118, comprising means for controlling reproducing for having said content key and said contents data encrypted by the content key reproduced from said record medium of said data storage apparatus to read them, and has a reproducing apparatus on which said data storage apparatus is mounted in a removable manner.

125. The recording and reproducing system according to claim 124, wherein said reproducing apparatus comprises means for decrypting contents, that is, decrypting by said content key said contents data encrypted by the content key read from said data storage apparatus.

126. The recording and reproducing system according to claim 124, wherein said means for controlling reproducing limits said data storage apparatus as to reproduction of said contents data encrypted by said content key recorded on said record medium.

127. The recording and reproducing system according to claim 126, wherein said limitation of reproduction is the number of times of possible reproduction of said contents data.

128. The recording and reproducing system according to claim 126, wherein said limitation of reproduction is the period of possible reproduction of said contents data.

129. The recording and reproducing system according to claim 118, wherein said means for holding a save key of said data storage apparatus stores said save key unique to said data storage apparatus.

130. A recording and reproducing apparatus to which a data storage apparatus having a predetermined record medium is provided in a removable manner, comprising:

means for sending out contents data encrypted by a predetermined content key and the content key to said data storage apparatus;

means for controlling recording and reproducing, that is, encrypting said content key by a predetermined save key and recording said contents data encrypted by said content key on said record medium, or reproducing said content key encrypted by said save key and said contents data encrypted by the content key from the record medium and decrypting by said save key said content key encrypted key by the save key; and

means for reading said content key and said contents data encrypted by the content key from said data storage apparatus.

131. The recording and reproducing apparatus according to claim 130, comprising means for decrypting contents, that is, decrypting by using said content key said contents data encrypted by the content key read from said data storage apparatus.

132. The recording and reproducing apparatus according to claim 130, wherein said means for controlling recording and reproducing limits said data storage apparatus as to reproduction of said contents data encrypted by said content key recorded on said record medium.

133. The recording and reproducing apparatus according to claim 132, wherein said limitation of reproduction is the number of times of possible reproduction of said contents data.

134. The recording and reproducing apparatus according to claim 132, wherein said limitation of reproduction is the period of possible reproduction of said contents data.

135. The recording and reproducing apparatus according to claim 130, wherein said means for controlling recording and reproducing encrypts or decrypts said content key by using said save key unique to said data storage apparatus.

136. A reproducing apparatus to which a data storage apparatus having a predetermined record medium is provided in a removable manner, comprising:

means for controlling reproducing, that is, reproducing contents data encrypted by a predetermined content key and said content key encrypted by a predetermined save key recorded in advance on said record medium, and decrypting by using said save key said content key encrypted by the save key; and

means for reading said content key and said contents data encrypted by the content key from said data storage apparatus.

137. The reproducing apparatus according to claim 136, comprising means for decrypting contents, that is, decrypting by using said content key said contents data encrypted by the content key read from said data storage apparatus.

138. A reproducing apparatus according to claim 136, wherein said means for controlling reproducing limits said data storage apparatus as to reproduction of said contents data encrypted by said content key recorded on said record medium.

139. The reproducing apparatus according to claim 138, wherein said limitation of reproduction is the number of times of possible reproduction of said contents data.

140. The reproducing apparatus according to claim 138, wherein said limitation of reproduction is the period of possible reproduction of said contents data.

141. The reproducing apparatus according to claim 136, wherein said means for controlling reproducing decrypts said content key by using said save key unique to said data storage apparatus.

142. A data storage apparatus provided to a recording and/or reproducing apparatus in a removable manner for recording and/or reproducing predetermined data under control of the recording and/or reproducing apparatus, comprising:

a predetermined record medium;

means for saving a predetermined save key;

means for communication for sending and receiving predetermined content data encrypted by a predetermined content key and the content key to and from said recording and/or reproducing apparatus;

means for encrypting said contents key by said save key under control of said recording and/or reproducing apparatus; and

means for recording and reproducing, that is, under control of said recording and/or reproducing apparatus, recording said content key encrypted by said save key and said contents data encrypted by the content key on said record medium or reproducing said content key

encrypted by said save key and said contents data encrypted by the content key from the record medium; and

means for decrypting by using said save key said content key encrypted by the save key under control of said recording and/or reproducing apparatus.

143. The data storage apparatus according to claim 142, wherein said means for holding a save key is tamper resistant.

144. The data storage apparatus according to claim 142, wherein said means for recording and reproducing limits reproduction of said contents data encrypted by said content key recorded on said record medium.

145. The data storage apparatus according to claim 144, wherein said limitation of reproduction is the number of times of possible reproduction of said contents data.

146. The data storage apparatus according to claim 144, wherein said limitation of reproduction is the period of possible reproduction of said contents data.

147. The data storage apparatus according to claim 142, wherein said means for recording and reproducing encrypts or decrypts said content key by using said save key unique to said data storage apparatus.

148. The recording and reproducing method of recording and reproducing predetermined contents data sent from an information sending apparatus on a removable data storage apparatus by a recording and reproducing apparatus, comprising:

a contents encrypting step of, by said information sending apparatus, encrypting said contents data by a predetermined content key;

a sending step of, by said information sending apparatus, sending said content key and said contents data encrypted by the content key;

a receiving step of, by said recording and reproducing apparatus, receiving said content key and said contents data encrypted by the content key sent from said information sending apparatus; and

a recording and reproducing controlling step of, by said recording and reproducing apparatus, sending out said content key and the contents data encrypted by the content key to said data storage apparatus and encrypting said content key by a save key held in advance on said data storage apparatus to record it on a record medium of said data storage apparatus together with said contents data encrypted by the content key, or reproducing said content key encrypted by said save key and said contents data encrypted by the content key from the record medium, and from said data storage apparatus, decrypting by said save key the content key encrypted by said save key to read it together with said contents data encrypted by said content key.

149. The recording and reproducing method according to claim 148, wherein said recording and reproducing controlling step uses for recording and reproducing said content key said save key held by predetermined tamper resistant means for holding a save key in said data storage apparatus.

150. The recording and reproducing method according to claim 148, wherein said recording and reproducing controlling step limits reproduction of said contents data encrypted by said content key recorded on said record medium of said data storage apparatus.

151. The recording and reproducing method according to claim 150, wherein said recording and reproducing controlling step limits the number of times of possible reproduction as limitation of reproduction of said contents data encrypted by said content key recorded on said record medium of said data storage apparatus.

152. The recording and reproducing method according to claim 150, wherein said recording and reproducing controlling step limits the period of possible reproduction as limitation of reproduction of said contents data encrypted by said content key recorded on said record medium of said data storage apparatus.

153. The recording and reproducing method according to claim 148, comprising a contents decrypting step of decrypting by using said

content key said contents data encrypted by the content key read from said data storage apparatus by said recording and reproducing apparatus.

154. The recording and reproducing method according to claim 148, wherein said recording and reproducing controlling step encrypts or decrypts said content key by using said save key unique to said data storage apparatus.

155. The recording and reproducing method according to claim 148, comprising a reproducing controlling step of, by a reproducing apparatus on which said data storage apparatus is mounted in a removable manner, reproducing and reading said content key and said contents data encrypted by the content key from said record medium of said data storage apparatus.

156. The recording and reproducing method according to claim 155, wherein said reproducing controlling step limits reproduction of said contents data encrypted by said content key recorded on said record medium of said data storage apparatus.

157. The recording and reproducing method according to claim 156, wherein said reproducing controlling step limits the number of times of possible reproduction as limitation of reproduction of said contents

data encrypted by said content key recorded on said record medium of said data storage apparatus.

158. The recording and reproducing method according to claim 156, wherein said reproducing controlling step limits the period of possible reproduction as limitation of reproduction of said contents data encrypted by said content key recorded on said record medium of said data storage apparatus.

159. The recording and reproducing method according to claim 156, comprising a contents decrypting step of decrypting by using said content key said contents data encrypted by the content key read from said data storage apparatus by said reproducing apparatus.

160. The recording and reproducing method according to claim 155, wherein said reproducing controlling step decrypts said content key by using said save key unique to said data storage apparatus.

161. A recording and reproducing method for recording and reproducing predetermined contents data on a record medium of a data storage apparatus provided in a removable manner to a recording and reproducing apparatus, comprising:

a sending out step of sending out contents data encrypted by a predetermined content key and the content key from said recording and reproducing apparatus to said data storage apparatus;

a recording and reproducing step of, under control of said recording and reproducing apparatus, encrypting said content key by a predetermined save key and recording said content key together with said contents data encrypted by said content key on said record medium, or reproducing said content key encrypted by said save key and said contents data encrypted by the content key from the record medium and decrypting by using said save key said content key encrypted by the save key; and

a reading step of reading said decrypted content key and said contents data encrypted by said content key from said data storage apparatus to said recording and reproducing apparatus.

162. The recording and reproducing method according to claim 161, comprising a contents decrypting step of decrypting by using said content key said contents data encrypted by the content key read from said data storage apparatus by said recording and reproducing apparatus.

163. The recording and reproducing method according to claim 161, wherein said recording and reproducing step limits reproduction of said contents data encrypted by said content key recorded on said record medium of said data storage apparatus under control of said recording and reproducing apparatus.

164. The recording and reproducing method according to claim 163, wherein said recording and reproducing step limits the number of times of possible reproduction as limitation of reproduction of said contents data encrypted by said content key recorded on said record medium of said data storage apparatus under control of said recording and reproducing apparatus.

165. The recording and reproducing method according to claim 163, wherein said recording and reproducing step limits the period of possible reproduction as limitation of reproduction of said contents data encrypted by said content key recorded on said record medium of said data storage apparatus under control of said recording and reproducing apparatus.

166. The recording and reproducing method according to claim 161, wherein said recording and reproducing step encrypts or decrypts said content key by using said save key unique to said data storage apparatus.

167. A reproducing method for reproducing predetermined contents data from a record medium of a data storage apparatus provided in a removable manner to a reproducing apparatus, comprising:

a reproducing step of, under control of said reproducing apparatus, reproducing contents data encrypted by a predetermined content key recorded in advance and said content key encrypted by a

predetermined save key from said record medium of said data storage apparatus;

a decrypting step of decrypting by using said save key said content key encrypted by the save key under control of said reproducing apparatus; and

a reading step of reading said content key and said contents data encrypted by said content key from said data storage apparatus to said reproducing apparatus.

168. The reproducing method according to claim 167, comprising a contents decrypting step of decrypting by using said content key said contents data encrypted by the content key read from said data storage apparatus by said reproducing apparatus.

169. The reproducing method according to claim 167, wherein said reproducing step limits reproduction of said contents data encrypted by said content key recorded on said record medium of said data storage apparatus under control of said reproducing apparatus.

170. The reproducing method according to claim 169, wherein said reproducing step limits the number of times of possible reproduction as limitation of reproduction of said contents data encrypted by said content key recorded on said record medium of said data storage apparatus under control of said reproducing apparatus.

171. The reproducing method according to claim 169, wherein said reproducing step limits the period of possible reproduction as limitation of reproduction of said contents data encrypted by said content key recorded on said record medium of said data storage apparatus under control of said reproducing apparatus.

172. The reproducing method according to claim 167, wherein said decrypting step decrypts said content key by using said save key unique to said data storage apparatus.

173. A program storage medium storing a predetermined program and supplying the program to a recording and reproducing apparatus, wherein said program comprises:

a sending out step of sending out contents data encrypted by a predetermined content key and the content key to a data storage apparatus provided in a removable manner to said recording and reproducing apparatus;

a recording and reproducing controlling step of controlling said data storage apparatus for encrypting said content key by a predetermined save key and recording it together with said contents data encrypted by said content key on a predetermined record medium of said data storage apparatus, or reproducing said content key encrypted by said save key and said contents data encrypted by the content key from the record medium and decrypting by using said save key said content key encrypted by the save key; and

a reading step of reading said decrypted content key and said contents data encrypted by said content key from said data storage apparatus.

174. The program storage medium according to claim 173, wherein said program comprises a contents decrypting step of decrypting by using said content key said contents data encrypted by the content key read from said data storage apparatus.

175. The program storage medium according to claim 173, wherein said recording and reproducing controlling step of said program limits reproduction of said contents data encrypted by said content key recorded on said record medium of said data storage apparatus under control of said recording and reproducing apparatus.

176. The program storage medium according to claim 175, wherein said recording and reproducing controlling step of said program limits the number of times of possible reproduction as limitation of reproduction of said contents data encrypted by said content key recorded on said record medium of said data storage apparatus under control of said recording and reproducing apparatus.

177. The program storage medium according to claim 175, wherein said recording and reproducing controlling step of said program limits the period of possible reproduction as limitation of reproduction of said

contents data encrypted by said content key recorded on said record medium of said data storage apparatus under control of said recording and reproducing apparatus.

178. The program storage medium according to claim 173, wherein said recording and reproducing controlling step of said program encrypts or decrypts said content key by using said save key unique to said data storage apparatus.

179. A program storage medium storing a predetermined program and supplying the program to a reproducing apparatus, characterized in that said program comprises:

a reproducing controlling step of controlling said data storage apparatus for reproducing contents data encrypted by a predetermined content key and said content key encrypted by a predetermined save key recorded in advance from the record medium of a data storage apparatus provided in a removable manner to said reproducing apparatus;

a decrypting controlling step of controlling said data storage apparatus for decrypting by using said save key said content key encrypted key by the save key; and

a reading step of reading said content key and said contents data encrypted by said content key from said data storage apparatus.

180. The program storage medium according to claim 179, wherein said program comprises a contents decrypting step of decrypting by using

said content key said contents data encrypted by said content key read from said data storage apparatus by said reproducing apparatus.

181. The program storage medium according to claim 179, wherein said reproducing controlling step of said program limits reproduction of said contents data encrypted by said content key recorded on said record medium of said data storage apparatus.

182. The program storage medium according to claim 181, wherein said reproducing controlling step of said program limits the number of times of possible reproduction as limitation of reproduction of said contents data encrypted by said content key recorded on said record medium of said data storage apparatus.

183. The program storage medium according to claim 181, wherein said reproducing controlling step of said program limits the period of possible reproduction as limitation of reproduction of said contents data encrypted by said content key recorded on said record medium of said data storage apparatus.

184. The program storage medium according to claim 179, wherein said decrypting controlling step of said program decrypts said content key by using said save key unique to said data storage apparatus.

185. A program storage medium storing a predetermined program and supplying the program to a data storage apparatus, wherein said program comprises:

a receiving step of receiving contents data encrypted by a predetermined content key and the content key sent from a recording and reproducing apparatus to which said data storage apparatus is provided in a removable manner;

a recording and reproducing step of, under control of said recording and reproducing apparatus, encrypting said content key by a predetermined save key and recording it together with said contents data encrypted by said content key on a predetermined record medium of said data storage apparatus, or reproducing said content key encrypted by said save key and said contents data encrypted by the content key from the record medium and decrypting by using said save key said content key encrypted key by the save key; and

a sending step of sending said content key and said contents data encrypted by said content key to said recording and reproducing apparatus.

186. The program storage medium according to claim 185, wherein said recording and reproducing step of said program limits reproduction of said contents data encrypted by said content key recorded on said record medium of said data storage apparatus under control of said recording and reproducing apparatus.

187. The program storage medium according to claim 186, wherein said recording and reproducing step of said program limits the number of times of possible reproduction as limitation of reproduction of said contents data encrypted by said content key recorded on said record medium of said data storage apparatus under control of said recording and reproducing apparatus.

188. The program storage medium according to claim 186, wherein said recording and reproducing step of said program limits the period of possible reproduction as limitation of reproduction of said contents data encrypted by said content key recorded on said record medium of said data storage apparatus under control of said recording and reproducing apparatus.

189. The program storage medium according to claim 185, wherein said recording and reproducing step of said program encrypts or decrypts said content key by using said save key unique to said data storage apparatus.

190. A program storage medium storing a predetermined program and supplying the program to a data storage apparatus, wherein said program comprises:

a reproducing step of, under control of a reproducing apparatus to which said data storage apparatus is provided in a removable manner, reproducing contents data encrypted by a predetermined content key and

said content key encrypted by a predetermined save key recorded in advance from the record medium of said data storage apparatus;

a decrypting step of decrypting by using said save key said content key encrypted by the save key under control of said reproducing apparatus; and

a sending step of sending said content key and said contents data encrypted by said content key to said reproducing apparatus.

191. The program storage medium according to claim 190, wherein said reproducing step of said program limits reproduction of said contents data encrypted by said content key recorded on said record medium under control of said reproducing apparatus.

192. The program storage medium according to claim 191, wherein said reproducing step of said program limits the number of times of possible reproduction as limitation of reproduction of said contents data encrypted by said content key recorded on said record medium under control of said reproducing apparatus.

193. The program storage medium according to claim 191, wherein said reproducing step of said program limits the period of possible reproduction as limitation of reproduction of said contents data encrypted by said content key recorded on said record medium under control of said reproducing apparatus.

194. The program storage medium according to claim 190, wherein said decrypting step of said program decrypts said content key by using said save key unique to said data storage apparatus.

195. A data management system, comprising:

a removable data storage apparatus having a predetermined record medium;

a recording apparatus for recording predetermined contents data on said record medium of said data storage apparatus; and

a management apparatus, connected to various apparatuses, for capturing contents data recorded on a record medium of said data storage apparatus and managing movement of the contents data to various apparatuses in place of said data storage apparatus.

196. The data management system according to claim 195, wherein said recording apparatus comprises:

means for sending said contents data encrypted by a predetermined content key, the content key, and handling policies prescribing the conditions for using the content key to said removable data storage apparatus; and

means for controlling recording, that is, controlling said data storage apparatus for prescribing the rights to utilize said contents data based on said handling policies and having license conditions information storing identification information for identifying a holder of the contents data created so as to record the license

conditions information, said contents data encrypted by said content key, the content key and said handling policies on said record medium; and

said management apparatus comprises:

means for capturing, that is, reproducing and capturing said contents data encrypted by said content key, the contents key, and said license conditions information from said record medium of said data storage apparatus; and

means for managing movement, that is, updating said license conditions information by changing said identification information, and moving said contents data encrypted by said content key and the content key together with said updated license conditions information to various apparatuses.

197. The data management system according to claim 196, wherein said means for capturing of said management apparatus captures said license conditions information, said contents data encrypted by said content key and the content key returned based on the license conditions information from said various apparatuses.

198. The data management system according to claim 196, wherein:

said means for controlling recording of said recording apparatus prescribes the rights to utilize said contents data based on said handling policies and has said license conditions information storing

said identification information unique to said data storage apparatus created; and

said means for managing movement of said management apparatus updates said license conditions information by changing said identification information unique to said data storage apparatus in said license conditions information to said identification information unique to said management apparatus.

199. The data management system according to claim 198, wherein:

said means for sending of said recording apparatus sends price information of said contents data in addition to said contents data encrypted by said content key, the content key, and said handling policies to said data storage apparatus;

said means for controlling recording has accounting information for purchase of said contents data generated by said data storage apparatus based on said handling policies and said price information to be held in a predetermined memory; and

said means for capturing of said management apparatus captures said accounting information together with said contents data encrypted by said content key, the contents key, and said license conditions information.

200. The data management system according to claim 199, wherein:

said means for capturing of said management apparatus captures said content key encrypted by a temporary key shared between said

management apparatus and said data storage apparatus and said accounting information encrypted by the temporary key.

201. The data management system according to claim 200, wherein:

said means for capturing of said management apparatus captures said accounting information to which signature data is added after being encrypted by said temporary key from said data storage apparatus.

202. A management apparatus connecting various apparatuses with a predetermined removable data storage apparatus, comprising:

means for capturing, that is, reproducing and capturing predetermined contents data recorded on a record medium of said data storage apparatus; and

means for managing movement of said contents data to various apparatuses in place of said data storage apparatus.

203. The management apparatus according to claim 202, wherein:

said means for capturing captures said contents data encrypted by a predetermined content key, the content key, and license conditions information prescribing the rights to utilize said contents data generated based on handling policies prescribing the conditions for using the content key and storing identification information for identifying a holder of the contents data from said record medium of said data storage apparatus; and

said means for managing movement updates said license conditions information by changing said identification information, and moves said contents data encrypted by said content key and the content key together with said updated license conditions information to various apparatuses.

204. The management apparatus according to claim 202, wherein:

said means for capturing captures the license conditions information, said contents data encrypted by said contents key and the content key returned from said various apparatuses based on said license conditions information.

205. The management apparatus according to claim 203, wherein:

said means for capturing captures said license conditions information storing said identification information unique to said data storage apparatus; and

said means for managing movement updates said license conditions information by changing said identification information unique to said data storage apparatus in said license conditions information to said identification information unique to said management apparatus.

206. The management apparatus according to claim 205, wherein:

said means for capturing captures accounting information for purchase of said contents data generated based on said handling policies

and price information of said contents data from said data storage apparatus.

207. The management apparatus according to claim 206, comprising means for decrypting by a temporary key predetermined data encrypted by the temporary key shared between said management apparatus and said data storage apparatus; and wherein:

said means for capturing captures said content key encrypted by said temporary key and said accounting information encrypted by the temporary key from said data storage apparatus; and

said means for decrypting decrypts by said temporary key said content key and said accounting information encrypted by said temporary key respectively.

208. The management apparatus according to claim 207, comprising means for detecting, that is, verifying signature data added to predetermined data and detecting whether or not said data is tampered; and wherein:

said means for capturing captures said accounting information to which signature data is added after being encrypted by said temporary key from said data storage apparatus; and

said means for detecting verifies said signature added to said accounting information encrypted by said temporary key.

209. A removable data storage apparatus having a predetermined record medium, comprising:

means for receiving contents data encrypted by a predetermined content key, the content key, and handling policies prescribing the conditions for using the content key sent from a predetermined recording apparatus when connected to the recording apparatus;

means for creating information, that is, creating license conditions information prescribing the rights to utilize said contents data based on said handling policies and storing identification information for identifying a holder of the contents data under control of said recording apparatus;

means for recording on said record medium said license conditions information, said contents data encrypted by said content key, the contents key and said handling policies under control of said recording apparatus;

means for, when connected to a management apparatus for managing movement of said contents data to various apparatuses, reproducing said contents data encrypted by said content key, the content key and said license conditions information from said record medium under control of said management apparatus; and

means for sending to said management apparatus said license conditions information for managing said contents data together with said contents data encrypted by said content key and the content key so as to shift management of said contents data under control of said management apparatus.

210. The data storage apparatus according to claim 209, wherein:

said means for creating information creates license conditions information for prescribing the rights to utilize said contents data based on said handling policies and storing changeable identification information for identifying a holder of the contents data.

211. The data storage apparatus according to claim 210, wherein:

said means for creating information creates said license conditions information storing said identification information unique to said data storage apparatus.

212. The data storage apparatus according to claim 211, wherein:

said means for receiving receives contents data encrypted by said content key, the content key and price information of said contents data sent together with said handling policies from said recording apparatus; and

said means for creating information creates accounting information for purchase of said contents data based on said handling policies and said price information and records it in a predetermined memory.

213. The data storage apparatus according to claim 212, wherein:

said means for creating information records said accounting information in said memory that is tamper resistant.

214. The data storage apparatus according to claim 213, comprising means for encrypting said content key by a temporary key shared with said management apparatus and also encrypting said accounting information by the temporary key; and

said means for sending sends to said management apparatus said content key encrypted by said temporary key and said accounting information encrypted by said temporary key together with said contents data encrypted by said content key and said license conditions information.

215. The data storage apparatus according to claim 214, comprising means for adding signature data for verifying whether or not tampering is performed to said accounting information encrypted by said temporary key; and wherein:

said means for sending sends to said management apparatus said accounting information encrypted by said temporary key with signature data added together with said contents data encrypted by said content key, said license conditions information and said content key encrypted by said temporary key.

216. A data management method, comprising:

a sending step of sending predetermined contents data to a removable data storage apparatus by a predetermined recording apparatus;

a recording step of recording said contents data on a record medium of said data storage apparatus under control of said recording apparatus;

a capturing step of reproducing and capturing said contents data from the record medium of said data storage apparatus by a management apparatus connected to various apparatuses; and

a movement managing step of managing movement of said contents data to various apparatuses by a management apparatus in place of said data storage apparatus.

217. The data management method according to claim 216, wherein:

said sending step sends to said data storage apparatus said contents data encrypted by a predetermined content key, the content key and handling policies prescribing conditions for using the content key;

said recording step records on said record medium said contents data encrypted by said content key, the content key and handling policies prescribing conditions for using the content key, and also has license conditions information prescribing the rights to utilize said contents data based on said handling policies and storing identification information for identifying a holder of the contents data created by said data storage apparatus and records it on said record medium;

said capturing step reproduces and captures said contents data encrypted by said content key, the content key and said license

conditions information from said record medium of said data storage apparatus; and

said movement managing step updates said license conditions information by changing said identification information, and moves said contents data encrypted by said content key and the content key together with said updated license conditions information to said various apparatuses.

218. The data management method according to claim 217, comprising:

a capturing step of capturing the license conditions information, said contents data encrypted by said content key and the content key returned from said various apparatuses based on said identification information by said management apparatus.

219. The data management method according to claim 217, wherein:

said recording step creates said license conditions information prescribing the rights to utilize said contents data based on said handling policies and storing said identification information unique to said data storage apparatus; and

said movement managing step updates said license conditions information by changing said identification information unique to said data storage apparatus in said license conditions information to said identification information unique to said management apparatus.

220. The data management method according to claim 219, wherein:

said sending step sends to said data storage apparatus price information of said contents data in addition to said contents data encrypted by said content key, the content key and said handling policies from said recording apparatus;

said recording step has accounting information for purchase of said contents data generated by said data storage apparatus based on said handling policies and said price information and holds it in a predetermined memory; and

said capturing step captures said accounting information together with said contents data encrypted by said content key, the contents key, and said license conditions information.

221. The data management method according to claim 220, wherein:

said capturing step captures, after being reproduced from said record medium of said data storage apparatus, said content key encrypted by a temporary key shared between said management apparatus and said data storage apparatus and said accounting information encrypted by the temporary key.

222. The data management system according to claim 221, wherein:

said capturing step captures said accounting information to which signature data is added after being encrypted by said temporary key from said data storage apparatus.

223. A data management method wherein various apparatuses are connected with a predetermined removable data storage apparatus, comprising:

a capturing step of reproducing and capturing predetermined contents data recorded on a record medium of said data storage apparatus; and

a movement managing step of managing movement of said contents data to various apparatuses in place of said data storage apparatus.

224. The data management method according to claim 223, wherein:

said capturing step captures said contents data encrypted by a predetermined content key, the content key, and license conditions information prescribing the rights to utilize said contents data generated based on handling policies prescribing the conditions for using the content key and storing identification information for identifying a holder of the contents data from said record medium of said data storage apparatus; and

said movement managing step updates said license conditions information by changing said identification information, and moves said contents data encrypted by said content key and the content key together with said updated license conditions information to said various apparatuses.

225. The data management method according to claim 223, wherein:

said capturing step captures the license conditions information, said contents data encrypted by said contents key and the content key returned from said various apparatuses based on said license conditions information.

226. The data management method according to claim 224, wherein:

said capturing step captures said license conditions information storing said identification information unique to said data storage apparatus; and

said movement managing step updates said license conditions information by changing said identification information unique to said data storage apparatus in said license conditions information to said identification information unique to said management apparatus.

227. The data management method according to claim 226, wherein:

said capturing step captures accounting information for purchase of said contents data generated based on said handling policies and price information of said contents data from said data storage apparatus.

228. The data management method according to claim 227, comprising:

a decrypting step of decrypting by a temporary key predetermined data encrypted by the temporary key shared between said management apparatus and said data storage apparatus; and wherein:

said capturing step captures said content key encrypted by said temporary key and said accounting information encrypted by the temporary key from said data storage apparatus; and

said decrypting step decrypts by said temporary key said content key and said accounting information encrypted by said temporary key respectively.

229. The data management method according to claim 228, comprising a detecting step of verifying signature data added to predetermined data and detecting whether or not said data is tampered; and wherein:

said capturing step captures said accounting information to which signature data is added after being encrypted by said temporary key from said data storage apparatus; and

said detecting step verifies said signature added to said accounting information encrypted by said temporary key.

230. A data management and movement method for a removable data storage apparatus having a predetermined record medium, comprising:

a receiving step of receiving contents data encrypted by a predetermined content key, the content key, and handling policies prescribing the conditions for using the content key sent from a predetermined recording apparatus to said data storage apparatus;

an information creating step of creating license conditions information prescribing the rights to utilize said contents data based on said handling policies and storing identification information for

identifying a holder of the contents data under control of said recording apparatus;

a recording step of recording on said record medium said license conditions information, said contents data encrypted by said content key, the contents key and said handling policies under control of said recording apparatus;

a reproducing step of, when said data storage apparatus is connected to a management apparatus for managing movement of said contents data to various apparatuses, reproducing said contents data encrypted by said content key, the content key and said license conditions information from said record medium under control of the management apparatus; and

a sending step of sending to said management apparatus said license conditions information for managing said contents data together with said contents data encrypted by said content key and the content key from said data storage apparatus so as to shift management of said contents data under control of said management apparatus.

231. The data management and movement method according to claim 230, wherein:

said information creating step creates license conditions information for prescribing the rights to utilize said contents data based on said handling policies and storing changeable identification information for identifying a holder of the contents data.

232. The data management and movement method according to claim 231, wherein:

said information creating step creates said license conditions information storing said identification information unique to said data storage apparatus.

233. The data management and movement method according to claim 232, wherein:

said receiving step receives contents data encrypted by said content key, the content key and price information of said contents data sent together with said handling policies from said recording apparatus; and

said information creating step creates accounting information for purchase of said contents data based on said handling policies and said price information and records it in a predetermined memory.

234. The data management and movement method according to claim 233, wherein:

said information creating step records said accounting information in said memory that is tamper resistant.

235. The data management and movement method according to claim 234, comprising:

an encrypting step of encrypting said content key by a temporary key shared with said management apparatus and also encrypting said accounting information by the temporary key; and wherein:

said sending step sends to said management apparatus said content key encrypted by said temporary key and said accounting information encrypted by said temporary key together with said contents data encrypted by said content key and said license conditions information.

236. The data management and movement method according to claim 235, comprising:

an adding step of adding signature data for verifying whether or not tampering is performed to said accounting information encrypted by said temporary key; and wherein:

said sending step sends to said management apparatus said accounting information encrypted by said temporary key with signature data added together with said contents data encrypted by said content key, said license conditions information and said content key encrypted by said temporary key.

237. A program storage medium storing a predetermined program and supplying the program to a management apparatus, characterized in that said program comprises:

a capturing step of reproducing and capturing predetermined contents data from a record medium of a predetermined removable data

storage apparatus connected to said management apparatus to which various apparatuses will be connected; and

a movement managing step of managing movement of said contents data to various apparatuses in place of said data storage apparatus.

238. The program storage medium according to claim 237, wherein:

said capturing step captures said contents data encrypted by a predetermined content key, the content key, and license conditions information prescribing the rights to utilize said contents data generated based on handling policies prescribing the conditions for using the content key and storing identification information for identifying a holder of the contents data from said record medium of said data storage apparatus; and

said movement managing step updates said license conditions information by changing said identification information, and moves said contents data encrypted by said content key and the content key together with said updated license conditions information to said various apparatuses.

239. The program storage medium according to claim 237, wherein:

said capturing step of said program captures the license conditions information, said contents data encrypted by said contents key and the content key returned from said various apparatuses based on said license conditions information.

240. The program storage medium according to claim 238, wherein:

said capturing step of said program captures said license conditions information storing said identification information unique to said data storage apparatus; and

said movement managing step updates said license conditions information by changing said identification information unique to said data storage apparatus in said license conditions information to said identification information unique to said management apparatus.

241. The program storage medium according to claim 240, wherein:

said capturing step of said program captures accounting information for purchase of said contents data generated based on said handling policies and price information of said contents data from said data storage apparatus.

242. The program storage medium according to claim 241, wherein said program comprises a decrypting step of decrypting predetermined data encrypted by a temporary key shared between said management apparatus and said data storage apparatus by the temporary key; and

said capturing step captures said content key encrypted by said temporary key and said accounting information encrypted by the temporary key from said data storage apparatus; and

said decrypting step decrypts by said temporary key said content key and said accounting information encrypted by said temporary key respectively.

243. The program storage medium according to claim 242, wherein said program comprises a detecting step of verifying signature data added to predetermined data and detecting whether or not said data is tampered; and

said capturing step captures said accounting information to which signature data is added after being encrypted by said temporary key from said data storage apparatus; and

said detecting step verifies said signature added to said accounting information encrypted by said temporary key.

244. A program storage medium storing a predetermined program and supplying the program to a data storage apparatus, characterized in that said program comprises:

a receiving step of receiving contents data encrypted by a predetermined content key, the content key, and handling policies prescribing the conditions for using the content key sent from a predetermined recording apparatus to said removable data storage apparatus;

an information creating step of creating license conditions information prescribing the rights to utilize said contents data based on said handling policies and storing identification information for identifying a holder of the contents data under control of said recording apparatus;

a recording step of recording on a predetermined record medium said license conditions information, said contents data encrypted by said content key, the contents key and said handling policies under control of said recording apparatus;

a reproducing step of, when said data storage apparatus is connected to a management apparatus for managing movement of said contents data to various apparatuses, reproducing said contents data encrypted by said content key, the content key and said license conditions information from said record medium under control of the management apparatus; and

a sending step of sending to said management apparatus said license conditions information for managing said contents data together with said contents data encrypted by said content key and the content key from said data storage apparatus so as to shift management of said contents data under control of said management apparatus.

245. The program storage medium according to claim 244, wherein:

said information creating step of said program creates license conditions information for prescribing the rights to utilize said contents data based on said handling policies and storing changeable identification information for identifying a holder of the contents data.

246. The program storage medium according to claim 245, wherein:

said information creating step of said program creates said license conditions information storing said identification information unique to said data storage apparatus.

247. The program storage medium according to claim 246, wherein:

said receiving step of said program receives contents data encrypted by said content key, the content key and price information of said contents data sent together with said handling policies from said recording apparatus; and

said information creating step creates accounting information for purchase of said contents data based on said handling policies and said price information and records it in a predetermined memory.

248. The program storage medium according to claim 247, wherein:

said information creating step of said program records said accounting information in said memory that is tamper resistant.

249. The program storage medium according to claim 248, wherein said program comprises an encrypting step of encrypting said content key by a temporary key shared with said management apparatus and also encrypting said accounting information by the temporary key; and

said sending step sends to said management apparatus said content key encrypted by said temporary key and said accounting information encrypted by said temporary key together with said contents data encrypted by said content key and said license conditions information.

250. The program storage medium according to claim 249, wherein said program comprises an adding step of adding signature data for verifying whether or not tampering is performed to said accounting information encrypted by said temporary key; and

said sending step sends to said management apparatus said accounting information encrypted by said temporary key with signature data added together with said contents data encrypted by said content key, said license conditions information and said content key encrypted by said temporary key.

251. An information provision system constructed of an information receiving apparatus and said regulating apparatus, wherein said information receiving apparatus comprises:

means on the receiving apparatus side for receiving predetermined contents data;

means for adding a signature to utilization permission data showing said received contents data;

means on the receiving apparatus side for sending said utilization permission data to which said signature is added; and

said information regulating apparatus comprises:

means on the regulating apparatus side for receiving said utilization permission data to which said signature is added;

means for determining, that is, verifying said signature added to said utilization permission data to determine whether or not the utilization permission data is illegal data; and

means for notifying said information receiving apparatus, if determined as a result of verifying said signature that said utilization permission data is illegal data, of nonpermission of utilization of said contents data and prohibiting said information receiving apparatus from utilizing said contents data.

252. The information provision system according to claim 251, wherein:

said means for determining of said information regulating apparatus verifies a signature on said utilization permission data, and determines that said utilization permission data is illegal data if the utilization permission data is tampered to show contents data different from said contents data received by said information receiving apparatus.

253. The information provision system according to claim 252, wherein:

said means for adding of said information receiving apparatus adds said signature to said utilization permission data prescribing the rights to utilize said contents data; and

said means for determining of said information regulating apparatus verifies said signature on said utilization permission data, and determines that said utilization permission data is illegal data

if said utilization rights prescribed by the utilization permission data are tampered to prescribe other utilization rights.

254. The information provision system according to claim 253, comprising an information sending apparatus for sending said contents data; and wherein:

said information receiving apparatus and said information regulating apparatus are connected online via said information sending apparatus.

255. An information regulating apparatus connected online with a predetermined information receiving apparatus, comprising:

means for receiving utilization permission data showing predetermined contents data and to which a signature is added sent from said information receiving apparatus;

means for determining, that is, verifying the signature on said utilization permission data to determine whether or not the utilization permission data is illegal data; and

means for notifying said information receiving apparatus, if determined that said utilization permission data is illegal data as a result of verifying said signature, of nonpermission of utilization of said contents data and prohibiting said information receiving apparatus from utilizing said contents data.

256. The information regulating apparatus according to claim 255, wherein:

said means for determining verifies a signature on said utilization permission data, and determines that said utilization permission data is illegal data if the utilization permission data is tampered to show contents data different from said contents data received by said information receiving apparatus.

257. The information regulating apparatus according to claim 256, wherein:

said means for receiving receives said utilization permission data prescribing the rights to utilize said contents data and to which said signature is added; and

said means for determining verifies a signature on said utilization permission data, and determines that said utilization permission data is illegal data if said utilization rights are tampered to prescribe other utilization rights.

258. The information regulating apparatus according to claim 255, wherein:

said means for receiving receives accounting information generated during a purchasing process of said contents data and to which said signature is added as said utilization permission data;

said means for determining verifies the signature on said accounting information to determine whether or not said accounting information is illegal data; and

said means for notifying notifies said information receiving apparatus, if determined that said accounting information is illegal data since it is tampered as a result of verifying said signature, of suspension of the purchasing process as nonpermission of utilization of said contents data and prohibits said information receiving apparatus from purchasing said contents data.

259. The information regulating apparatus according to claim 258, comprising a means for decrypting predetermined encrypted data; and wherein:

said means for receiving receives said accounting information to which said signature is added after being encrypted by a temporary key shared between said information regulating apparatus and said information receiving apparatus;

said means for determining verifies the signature on said accounting information to determine whether or not said accounting information is illegal data; and

said means for decrypting decrypts said encrypted accounting information by said temporary key if it is determined that said accounting information is justifiable data as a result of verifying said signature.

260. An information receiving apparatus connected online to a predetermined information regulating apparatus, comprising:

means for receiving predetermined contents data that is sent;

means for adding to utilization permission data showing said contents data a signature capable of detecting whether or not said contents data shown by the utilization permission data is tampered to be other contents data; and

means for sending said utilization permission data to which said signature is added to said information regulating apparatus which decides whether or not to prohibit utilization of said contents data according to the result of verification of said signature.

261. The information receiving apparatus according to claim 260, wherein:

said means for adding adds said signature in order to allow detection of whether or not said utilization permission data prescribing the rights to utilize said contents data is tampered to prescribe other utilization rights.

262. The information receiving apparatus according to claim 260, comprising means for processing purchase, that is, performing a purchasing process of said contents data and generating accounting information for purchase of said contents data; and wherein:

said means for adding adds said signature to said accounting information generated during a purchasing process of said contents data as said utilization permission data.

263. The information receiving apparatus according to claim 262, comprising means for receiving a notice of whether or not utilization of said contents data is prohibited from said information regulating apparatus; and wherein:

said means for processing purchase suspends said purchasing process if notified of nonpermission of utilization of said contents data from said information receiving apparatus during a purchasing process of said contents data.

264. The information receiving apparatus according to claim 263, comprising means for encrypting said accounting information by a temporary key shared with said information regulating apparatus; and wherein:

said means for adding adds said signature to said accounting information encrypted as above.

265. The information receiving apparatus according to claim 260, comprising means for connecting online to said information regulating apparatus via a predetermined information sending apparatus sending said contents data.

266. An information provision method, comprising:

a sending step of, by an information receiving apparatus, receiving predetermined contents data, adding a signature to utilization permission data showing the received contents data and sending it;

a utilization prohibiting step of, by an information regulating apparatus, verifying a signature on said utilization permission data to determine whether or not the utilization permission data is illegal data, and prohibiting the information receiving apparatus from utilizing said contents data if it determines that the data is illegal data.

267. The information provision method according to claim 266, wherein:

said utilization prohibiting step verifies a signature on said utilization permission data, and determines that said utilization permission data is illegal data if the utilization permission data is tampered to show contents data different from said contents data received by said information receiving apparatus.

268. The information provision method according to claim 267, wherein:

said sending step adds said signature to said utilization permission data prescribing the rights to utilize said contents data and sends it; and

said utilization prohibiting step verifies a signature on said utilization permission data, and determines that said utilization

permission data is illegal data if said utilization rights prescribed by said data is tampered to prescribe other utilization rights.

269. The information provision method according to claim 268, wherein:

said sending step sends said utilization permission data to said information regulating apparatus to which said information receiving apparatus is connected online via an information sending apparatus sending said contents data.

270. An information regulating method by an information regulating apparatus connected online with a predetermined information receiving apparatus, comprising:

a receiving step of receiving utilization permission data showing predetermined contents data and to which a signature is added sent from said information receiving apparatus;

a determining step of verifying the signature on said utilization permission data to determine whether or not the utilization permission data is illegal data; and

a notifying step of notifying said information receiving apparatus, if it determines that said utilization permission data is illegal data as a result of verifying said signature, of nonpermission of utilization of said contents data and prohibiting said information receiving apparatus from utilizing said contents data.

271. The information regulating method according to claim 270, wherein:

said means for determining verifies a signature on said utilization permission data, and determines that said utilization permission data is illegal data if the utilization permission data is tampered to show contents data different from said contents data received by said information receiving apparatus.

272. The information regulating method according to claim 271, wherein:

said receiving step receives said utilization permission data prescribing the rights to utilize said contents data and to which said signature is added; and

said determining step verifies a signature on said utilization permission data, and determines that said utilization permission data is illegal data if said utilization rights are tampered to prescribe other utilization rights.

273. The information regulating method according to claim 270, wherein:

said receiving step receives accounting information generated during a purchasing process of said contents data and to which said signature is added as said utilization permission data;

said determining step verifies the signature on said accounting information to determine whether or not said accounting information is illegal data; and

said notifying step notifies said information receiving apparatus, if it determines that said accounting information is illegal data since it is tampered as a result of verifying said signature, of suspension of the purchasing process as nonpermission of utilization of said contents data and prohibits said information receiving apparatus from purchasing said contents data.

274. The information regulating method according to claim 273, comprising a decrypting step of decrypting predetermined encrypted data; and wherein:

said receiving step receives accounting information to which said signature is added after being encrypted by a temporary key shared between said information regulating apparatus and said information receiving apparatus;

said determining step verifies the signature on said accounting information to determine whether or not said accounting information is illegal data; and

said decrypting step decrypts said encrypted accounting information by said temporary key if it is determined that said accounting information is justifiable data as a result of verifying said signature.

275. A data utilization method for utilizing predetermined contents data by an information receiving apparatus connected online to a predetermined information regulating apparatus, comprising:

a receiving step of receiving predetermined contents data that is sent;

an adding step of adding to utilization permission data showing said contents data a signature capable of detecting whether or not said contents data shown by the utilization permission data is tampered to be other contents data; and

a sending step of sending said utilization permission data to which said signature is added to said information regulating apparatus which decides whether or not to prohibit utilization of said contents data according to the result of verification of said signature.

276. An data utilization method according to claim 275, wherein:

said adding step adds said signature in order to allow detection of whether or not said utilization permission data prescribing the rights to utilize said contents data is tampered to prescribe other utilization rights.

277. The data utilization method according to claim 275, comprising a purchase processing step of performing a purchasing process of said contents data and generating accounting information for purchase of said contents data; and wherein:

said adding step adds said signature to said accounting information generated during a purchasing process of said contents data as said utilization permission data.

278. The data utilization method according to claim 277, comprising a receiving step of receiving a notice of whether or not utilization of said contents data is prohibited from said information regulating apparatus; and wherein:

said purchase processing step suspends said purchasing process if notified of nonpermission of utilization of said contents data from said information receiving apparatus during a purchasing process of said contents data.

279. The data utilization method according to claim 278, comprising an encrypting step of encrypting said accounting information by a temporary key shared with said information regulating apparatus; and wherein:

said means for adding adds said signature to said accounting information encrypted as above.

280. The data utilization method according to claim 275, comprising a connecting step of being connected online to said information regulating apparatus via a predetermined information sending apparatus sending said contents data.

281. A program storage medium storing a predetermined program and supplying the program to an information regulating apparatus, characterized in that said program comprises:

a receiving step of receiving utilization permission data showing predetermined contents data and to which a signature is added sent from said information receiving apparatus connected online;

a determining step of verifying the signature on said utilization permission data to determine whether or not the utilization permission data is illegal data; and

a notifying step of notifying said information receiving apparatus, if it determines that said utilization permission data is illegal data as a result of verifying said signature, of nonpermission of utilization of said contents data and prohibiting said information receiving apparatus from utilizing said contents data.

282. The program storage medium according to claim 281, wherein:

said determining step of said program verifies a signature on said utilization permission data, and determines that said utilization permission data is illegal data if the utilization permission data is tampered to show contents data different from said contents data received by said information receiving apparatus.

283. The program storage medium according to claim 282, wherein:

said receiving step of said program receives said utilization permission data prescribing the rights to utilize said contents data and to which said signature is added; and

said determining step verifies a signature on said utilization permission data, and determines that said utilization permission data is illegal data if said utilization rights are tampered to prescribe other utilization rights.

284. The program storage medium according to claim 281, wherein:

said receiving step of said program receives accounting information generated during a purchasing process of said contents data and to which said signature is added as said utilization permission data;

said determining step verifies the signature on said accounting information to determine whether or not said accounting information is illegal data; and

said notifying step notifies said information receiving apparatus, if it determines that said accounting information is illegal data since it is tampered as a result of verifying said signature, of suspension of the purchasing process as nonpermission of utilization of said contents data and prohibits said information receiving apparatus from purchasing said contents data.

285. The program storage medium according to claim 284, wherein said program comprises a decrypting step of decrypting predetermined encrypted data; and wherein:

said receiving step receives said accounting information to which said signature is added after being encrypted by a temporary key shared between said information regulating apparatus and said information receiving apparatus;

said determining step verifies the signature on said accounting information to determine whether or not said accounting information is illegal data; and

said decrypting step decrypts said encrypted accounting information by said temporary key if it is determined that said accounting information is justifiable data as a result of verifying said signature.

286. A program storage medium for storing a predetermined program and supplying the program to an information receiving apparatus, characterized in that said program comprises:

a receiving step of receiving predetermined contents data by an information receiving apparatus connected online to a predetermined information regulating apparatus;

an adding step of adding to utilization permission data showing said contents data a signature capable of detecting whether or not said contents data shown by the utilization permission data is tampered to be other contents data; and

a sending step of sending said utilization permission data to which said signature is added to said information regulating apparatus which decides whether or not to prohibit utilization of said contents data according to the result of verification of said signature.

287. The program storage medium according to claim 286, wherein:

said adding step of said program adds said signature in order to allow detection of whether or not said utilization permission data prescribing the rights to utilize said contents data is tampered to prescribe other utilization rights.

288. The program storage medium according to claim 286, wherein said program comprises a purchase processing step of performing a purchasing process of said contents data and generating accounting information for purchase of said contents data; and

said adding step adds said signature to said accounting information generated during a purchasing process of said contents data as said utilization permission data.

289. The program storage medium according to claim 288, wherein said program comprises a receiving step of receiving a notice of whether or not utilization of said contents data is prohibited from said information regulating apparatus; and

said purchase processing step suspends said purchasing process if notified of nonpermission of utilization of said contents data from

said information receiving apparatus during a purchasing process of said contents data.

290. The program storage medium according to claim 289, wherein said program comprises an encrypting step of encrypting said accounting information by a temporary key shared with said information regulating apparatus; and

said adding step adds said signature to said accounting information encrypted as above.

291. The program storage medium according to claim 286, wherein said program comprises a connecting step of being connected online to said information regulating apparatus via a predetermined information sending apparatus sending said contents data.

292. An information provision system supplying predetermined contents data sent from an information sending apparatus to an information provision apparatus, wherein said information sending apparatus comprises:

means for encrypting said contents data by a predetermined content key;

means for sending said content key and said contents data encrypted by the content key; and

said information provision apparatus comprises:

means for receiving said content key and said contents data encrypted by the content key sent from said information sending apparatus;

means for decrypting by said content key said contents data encrypted by the content key;

means for inserting a digital watermark, that is, inserting by a digital watermark predetermined information into the contents data decrypted by said content key; and

means for recording the contents data with said information inserted on a removable record medium.

293. The information provision system according to claim 292, wherein said means for inserting a digital watermark of said information provision apparatus inserts said information for limiting duplication into said contents data by said digital watermark.

294. The information provision system according to claim 292, wherein said information sending apparatus comprises means for generating handling policies prescribing conditions for using said contents key; and

said means for sending sends said handling policies together with said content key and said contents data encrypted by the content key; and

said information provision apparatus comprises:

means for creating license conditions information prescribing conditions for using said contents data based on said handling policies; and

means for storing, that is, sending said license conditions information together with said content key and said contents data encrypted by the content key to a predetermined removable data storage apparatus and storing them thereon.

295. The information provision system according to claim 294, wherein said means for storing of said information provision apparatus sends said handling policies together with said content key and said contents data encrypted by the content key to said data storage apparatus and stores them thereon, and creates said license conditions information by said data storage apparatus based on said handling policies and stores them thereon.

296. The information provision system according to claim 295, comprising a management apparatus for managing sending of said contents data from said information sending apparatus to said information provision apparatus; and wherein:

said means for storing of said information provision apparatus sends identification information for identifying said data storage apparatus to said management apparatus; and

said management apparatus manages said data storage apparatus storing said contents data based on said identification information.

297. An information provision apparatus supplying predetermined contents data sent from an information sending apparatus, comprising:

means for receiving said contents data encrypted by a predetermined content key and the content key sent from said information sending apparatus;

means for decrypting by said content key the contents data encrypted by the content key;

means for inserting a digital watermark, that is, inserting by a digital watermark predetermined information into said contents data decrypted by said content key; and

means for recording said contents data with said information inserted on a removable record medium.

298. The information provision apparatus according to claim 297, wherein said means for inserting a digital watermark inserts said information for limiting duplication into said contents data by said digital watermark.

299. The information provision apparatus according to claim 297, comprising:

means for creating license conditions information prescribing conditions for using said contents data based on the handling policies prescribing conditions for using said content key sent from said

information sending apparatus together with said content key and said contents data encrypted by the content key; and

means for storing, that is, sending said license conditions information together with said content key and said contents data encrypted by the content key to a predetermined removable data storage apparatus and storing them thereon.

300. The information provision apparatus according to claim 299, wherein said means for storing sends to said data storage apparatus said content key and said contents data encrypted by the content key and said handling policies and stores them thereon, and creates said license conditions information by said data storage apparatus based on said handling policies and stores them thereon.

301. An information provision apparatus providing predetermined contents data sent from an information sending apparatus, comprising:

means for creating license conditions information prescribing conditions for using said contents data based on the handling policies prescribing conditions for using said content key sent from said information sending apparatus together with said content key and said contents data encrypted by said content key; and

means for storing, that is, sending said license conditions information together with said content key and said contents data encrypted by said content key to said predetermined removable data storage apparatus and storing them thereon.

302. The information provision apparatus according to claim 301, wherein said means for storing sends to said data storage apparatus said content key, said contents data encrypted by the content key and said handling policies and stores them thereon, and creates said license conditions information by said data storage apparatus based on said handling policies and stores them thereon.

303. A removable data storage apparatus for storing predetermined contents data sent from an information provision apparatus, comprising:

a predetermined record medium;

means for receiving said content key, said contents data encrypted by the content key and license conditions information prescribing the conditions for using said contents data created as required based on the handling policies prescribing conditions for using said content key sent from said information provision apparatus; and

means for recording on said record medium said content key, said contents data encrypted by the content key and said license conditions information.

304. The data storage apparatus according to claim 303, comprising means for creating said license conditions information based on said handling policies sent from said information provision apparatus; wherein:

said means for recording records on said record medium said content key, said contents data encrypted by the content key and said license conditions information created by said means for creating said license conditions information when said content key, said contents data encrypted by the content key and said handling policies are sent from said information provision apparatus.

305. An information provision method for providing predetermined contents data sent from an information sending apparatus to an information provision apparatus, comprising:

a data sending step of sending a predetermined content key and said contents data encrypted by the content key by said information sending apparatus; and

a receiving step of receiving said content key and said contents data encrypted by the content key by said information provision apparatus;

a decrypting step of decrypting by said content key the contents data encrypted by said content key by said information provision apparatus;

a digital watermark inserting step of inserting by a digital watermark predetermined information into said contents data decrypted by said content key by said information provision apparatus; and

a data recording step of recording on a removable record medium said contents data with said information inserted by said information provision apparatus.

306. The information provision method according to claim 305, wherein said digital watermark inserting step inserts said information for limiting duplication into said contents data by said digital watermark.

307. The information provision method according to claim 305, comprising:

a handling policies generating step of generating handling policies prescribing conditions for using said contents key to be sent to said information provision apparatus by said information sending apparatus;

a license conditions information creating step of creating license conditions information prescribing conditions for using said contents data based on said handling policies by said information provision apparatus; and

a storing step of sending said license conditions information together with said content key and said contents data encrypted by the content key to a predetermined removable data storage apparatus and storing them thereon by said information provision apparatus.

308. The information provision method according to claim 307, wherein said storing step sends said handling policies together with said content key and said contents data encrypted by the content key to said data storage apparatus and stores them thereon, and creates said license

conditions information by said data storage apparatus based on said handling policies and stores them thereon.

309. The information provision method according to claim 308, comprising:

an identification information sending step of sending identification information for identifying said data storage apparatus to a management apparatus managing sending of said contents data from said information sending apparatus to said information provision apparatus by said information provision apparatus; and

a managing step of managing said data storage apparatus storing said contents data based on said identification information by said management apparatus.

310. An information provision method for providing predetermined contents data by an information provision apparatus, comprising:

a receiving step of receiving said contents data encrypted by a predetermined content key and the content key sent from an information sending apparatus;

a decrypting step of decrypting by said content key said contents data encrypted by the content key;

a digital watermark inserting step of inserting by a digital watermark predetermined information into said contents data decrypted by said content key; and

a data recording step of recording said contents data with said information inserted on a removable record medium.

311. The information provision method according to claim 310, wherein said digital watermark inserting step inserts said information for limiting duplication into said contents data by said digital watermark.

312. The information provision method according to claim 310, comprising:

a license conditions information creating step of creating license conditions information prescribing conditions for using said contents data based on handling policies prescribing conditions for using said content key sent from said information sending apparatus together with said content key and said contents data encrypted by the content key; and

a storing step of sending said license conditions information together with said content key and said contents data encrypted by the content key to a predetermined removable data storage apparatus and storing them thereon.

313. The information provision method according to claim 312, wherein said storing step sends to said data storage apparatus said content key, said contents data encrypted by the content key and said handling policies and stores them thereon, and creates said license conditions

information by said data storage apparatus based on said handling policies and stores them thereon.

314. An information provision method for providing predetermined contents data by an information provision apparatus, comprising:

a license conditions information creating step of creating license conditions information prescribing conditions for using said contents data based on handling policies prescribing conditions for using said content key sent from said information sending apparatus together with said content key and said contents data encrypted by the content key; and

a storing step of sending said license conditions information together with said content key and said contents data encrypted by the content key to a predetermined removable data storage apparatus and storing them thereon.

315. The information provision method according to claim 314, wherein said storing step sends to said data storage apparatus said content key, said contents data encrypted by the content key and said handling policies and stores them thereon, and creates said license conditions information by said data storage apparatus based on said handling policies and stores them thereon.

316. A data store method for storing predetermined contents data sent from an information provision apparatus on a removable data storage apparatus, comprising:

a receiving step of receiving said content key, said contents data encrypted by the content key and license conditions information prescribing conditions for using said contents data created as required based on handling policies prescribing conditions for using said content key sent from said information provision apparatus; and

a recording step of recording said content key, said contents data encrypted by the content key and said license conditions information on a record medium.

317. The data store method according to claim 316, comprising a license conditions information creating step of creating said license conditions information based on said handling policies sent from said information provision apparatus; wherein:

said recording step records on said record medium said content key, said contents data encrypted by the content key and said license conditions information created by said means for creating said license conditions information when only said content key, said contents data encrypted by the content key and said handling policies are sent from said information provision apparatus.

318. A program storage medium for storing a predetermined program and supplying the program to an information provision apparatus, wherein said program comprises:

a receiving step of receiving said contents data encrypted by a predetermined content key and the content key sent from said information sending apparatus;

a decrypting step of decrypting by said content key said contents data encrypted by the content key;

a digital watermark inserting step of inserting by a digital watermark predetermined information into said contents data decrypted by said content key; and

a data recording step of recording said contents data with said information inserted on a removable record medium.

319. The program storage medium according to claim 318, wherein said digital watermark inserting step of said program inserts said information for limiting duplication into said contents data by said digital watermark.

320. The program storage medium according to claim 318, wherein said program comprises:

a license conditions information creating step of creating license conditions information prescribing conditions for using said contents data based on said handling policies prescribing conditions for using said content key sent from said information sending apparatus

together with said content key and said contents data encrypted by the content key; and

a storing step of sending said license conditions information together with said content key and said contents data encrypted by the content key to a predetermined removable data storage apparatus and storing them thereon.

321. The program storage medium according to claim 320, wherein said storing step of said program sends to said data storage apparatus said content key, said contents data encrypted by the content key and said handling policies and stores them thereon, and creates said license conditions information by said data storage apparatus based on said handling policies and stores them thereon.

322. A program storage medium for storing a predetermined program and supplying the program to an information provision apparatus, wherein said program comprises:

a license conditions information creating step of creating license conditions information prescribing conditions for using said contents data based on handling policies prescribing conditions for using said content key sent from said information sending apparatus together with said content key and said contents data encrypted by the content key; and

a storing step of sending said license conditions information together with said content key and said contents data encrypted by the

content key to a predetermined removable data storage apparatus and storing them thereon.

323. The program storage medium according to claim 322, wherein said storing step of said program sends to said data storage apparatus said content key, said contents data encrypted by the content key and said handling policies and stores them thereon, and creates said license conditions information by said data storage apparatus based on said handling policies and stores them thereon.

324. A program storage medium for storing a predetermined program and supplying the program to a data storage apparatus, wherein said program comprises:

a receiving step of receiving said content key, said contents data encrypted by the content key and license conditions information prescribing conditions for using said contents data created as required based on handling policies prescribing conditions for using said content key sent from said information provision apparatus to said removable data storage apparatus; and

a recording step of recording said content key, said contents data encrypted by the content key and said license conditions information on a record medium.

325. The program storage medium according to claim 324, wherein said program comprises:

a license conditions information creating step of creating said license conditions information based on said handling policies sent from said information provision apparatus; wherein:

said recording step records on said record medium said content key, said contents data encrypted by the content key and said license conditions information created by said license conditions information creating step when only said content key, said contents data encrypted by the content key and said handling policies are sent from said information provision apparatus.

326. An information recording apparatus for storing predetermined contents data on a predetermined data storage apparatus, comprising:

a contents server holding a plurality of said contents data;

means for selecting, that is, managing each of said contents data held on said contents server by categorization, and if said category and the number of contents that are desired are specified, arbitrarily selecting a plurality of said contents data equivalent to said specified number of contents of said contents data belonging to said specified category; and

means for storing, that is, reading each of said selected contents data from said contents server and storing it on said data storage apparatus.

327. The information recording apparatus according to claim 326, comprising means for generating a random number based on said specified

number of contents; and wherein said means for selecting selects each of said contents data by using said random number.

328. The information recording apparatus according to claim 327, comprising means for creating license conditions information prescribing the rights to utilize each of said contents data selected by said means for selecting; and wherein:

said means for storing stores said license conditions information together with each of said contents data on said data storage apparatus.

329. The information recording apparatus according to claim 328, wherein said means for creating license conditions information creates said license conditions information prescribing said utilization rights so as to limit the number of times of reproduction of each of said contents data.

330. The information recording apparatus according to claim 328, wherein said means for creating license conditions information creates said license conditions information prescribing said utilization rights so as to limit the period of reproduction of each of said contents data.

331. The information recording apparatus according to claim 328, wherein said means for creating license conditions information creates

said license conditions information so as to store predetermined identification information; and

said means for storing detects said contents data to be deleted based on said identification information stored in said license conditions information and stores said contents data that is new so as to overwrite said detected contents data.

332. A data storage apparatus for storing predetermined contents data by an information recording apparatus, comprising:

a predetermined record medium;

means for receiving a plurality of said contents data belonging to said desired category and equivalent to said desired number of contents, of a plurality of said categorized contents data sent from said information recording apparatus;

means for recording each of said contents data collectively on said record medium.

333. The data storage apparatus according to claim 332, wherein said means for recording records on said record medium each of said contents data and said license conditions information prescribing the rights to utilize each of said contents data by sending said license conditions information together with each of said contents data from said information recording apparatus.

334. The data storage apparatus according to claim 333, wherein said means for recording records on said record medium said license conditions information prescribing said utilization rights so as to limit the number of times of reproduction of said contents data together with said contents data.

335. The data storage apparatus according to claim 333, wherein said means for recording records on said record medium said license conditions information prescribing said utilization rights so as to limit the period of reproduction of said contents data together with said contents data.

336. A data store method for storing predetermined contents data on a data storage apparatus by an information recording apparatus, comprising:

a selecting step of managing a plurality of said contents server held on a contents server in advance by categorization, and if said category and the number of contents that are desired are specified, arbitrarily selecting a plurality of said contents data equivalent to said specified number of contents, of said contents data belonging to said specified category; and

a storing step of reading each of said selected contents data from said contents server and storing it on said data storage apparatus.

337. The data store method according to claim 336, comprising a random number generating step of generating a random number based on said specified number of contents; and wherein:

said selecting step selects each of said contents data by using said random number.

338. The data store method according to claim 337, comprising a license conditions information creating step of creating license conditions information prescribing the rights to utilize each of said contents data selected by said step of selecting; and

said storing step stores said license conditions information together with each of said contents data on said data storage apparatus.

339. The data store method according to claim 338, wherein said license conditions information creating step creates said license conditions information prescribing said utilization rights so as to limit the number of times of reproduction of each of said contents data.

340. The data store method according to claim 338, wherein said license conditions information creating step creates said license conditions information prescribing said utilization rights so as to limit the period of reproduction of each of said contents data.

341. The data store method according to claim 338, wherein said license conditions information creating step creates said license conditions

information so as to store predetermined identification information; and

said storing step detects said contents data to be deleted based on said identification information stored in said license conditions information and stores said contents data that is new so as to overwrite said detected contents data.

342. A data store method for storing predetermined contents data on a data storage apparatus by an information recording apparatus, comprising:

a contents receiving step of receiving a plurality of said contents data belonging to said desired category and equivalent to said desired number of contents, of a plurality of said categorized contents data sent from said information recording apparatus to said data storage apparatus; and

a recording step of recording each of said contents data collectively on a record medium in said data storage apparatus.

343. The data store method according to claim 342, wherein said recording step records on said record medium each of said contents data and said license conditions information prescribing the rights to utilize each of said contents data by sending said license conditions information together with each of said contents data from said information recording apparatus.

344. The data store method according to claim 343, wherein said recording step records on said record medium said license conditions information prescribing said utilization rights so as to limit the number of times of reproduction of each of said contents data together with each of said contents data.

345. The data store method according to claim 343, wherein said recording step records on said record medium said license conditions information prescribing said utilization rights so as to limit the period of reproduction of each of said contents data together with each of said contents data.

346. A program storage medium for storing a predetermined program and supplying the program to an information recording apparatus, wherein said program comprises:

a selecting step of managing a plurality of said contents server held on a contents server in advance by categorization, and if said category and the number of contents that are desired are specified, arbitrarily selecting a plurality of said contents data equivalent to said specified number of contents, of a plurality of said contents data belonging to said specified category; and

a storing step of reading each of said selected contents data from said contents server and storing it on said data storage apparatus.

347. The program storage medium according to claim 346, wherein said program comprises a random number generating step of generating a random number based on said specified number of contents; and

said selecting step selects each of said contents data by using said random number.

348. The program storage medium according to claim 347, wherein said program comprises a license conditions information creating step of creating license conditions information prescribing the rights to utilize each of said contents data selected by said step of selecting; and

said storing step stores said license conditions information together with each of said contents data on said data storage apparatus.

349. The program storage medium according to claim 348, wherein said license conditions information creating step of said program creates said license conditions information prescribing said utilization rights so as to limit the number of times of reproduction of each of said contents data.

350. The program storage medium according to claim 348, wherein said license conditions information creating step of said program creates said license conditions information prescribing said utilization rights so as to limit the period of reproduction of each of said contents data.

351. The program storage medium according to claim 348, wherein said license conditions information creating step of said program creates said license conditions information so as to store predetermined identification information; and

said storing step detects said contents data to be deleted based on said identification information stored in said license conditions information and stores said contents data that is new so as to overwrite said detected contents data.

352. A program storage medium for storing a predetermined program and supplying the program to a data storage apparatus, wherein said program comprises:

a contents receiving step of receiving a plurality of said contents data belonging to said desired category and equivalent to a desired number of contents, of a plurality of said categorized contents data sent from an information recording apparatus; and

a recording step of recording each of said contents data collectively on a record medium.

353. The program storage medium according to claim 352, wherein said recording step of said program records on said record medium each of said contents data and said license conditions information prescribing the rights to utilize each of said contents data by sending said license

conditions information together with each of said contents data from said information recording apparatus.

354. The program storage medium according to claim 353, wherein said recording step of said program records on said record medium said license conditions information prescribing said utilization rights so as to limit the number of times of reproduction of each of said contents data together with each of said contents data.

355. The program storage medium according to claim 353, wherein said recording step of said program records on said record medium said license conditions information prescribing said utilization rights so as to limit the period of reproduction of each of said contents data together with each of said contents data.

356. An information provision system constructed of an information sending apparatus, an information receiving apparatus and a list sending apparatus, wherein:

said information sending apparatus comprises:

means for sending predetermined contents data; and

said list sending apparatus comprises:

means for creating a provision prohibition list showing said contents data designated as provision-prohibited; and

means for sending said prohibition list; and

said information receiving apparatus comprises:

means for receiving said contents data and said provision prohibition list;

means for determining whether or not said contents data sent from said information sending apparatus is provision-prohibited based on said provision prohibition list; and

means for stopping capture of the contents data in the case where said contents data is provision-prohibited according to results of determination acquired from said means for determining.

357. The information provision system according to claim 356, wherein said list sending apparatus comprises a means for registering said information sending apparatus designated as utilization-prohibited on said provision prohibition list;

said means for determining of said information receiving apparatus determines whether or not said contents data sent from said information sending apparatus is provision-prohibited as above and also determines whether or not said information sending apparatus is utilization-prohibited as above based on said provision prohibition list; and

said means for stopping capture stops capture of said contents data in the case where said contents data is provision-prohibited as above and in the case where said information sending apparatus is utilization-prohibited as above according to results of determination acquired from said means for determining respectively.

358. The information provision system according to claim 357, wherein:

said information receiving apparatus comprises:

one or more online apparatuses connected online to said list sending apparatus and receiving said provision prohibition list; and

one or more offline apparatuses not connected online to said list sending apparatus; and

said online apparatus comprises:

means for an online apparatus for sending a list, that is, sending said provision prohibition list to said offline apparatus on connecting the offline apparatus;

means for an online apparatus for receiving, that is, directly receiving said contents data sent from said information sending apparatus, or receiving said contents data sent from said information sending apparatus via other online apparatus and offline apparatus; and

means for an online apparatus for stopping capture of said contents data as required based on said provision prohibition list; and

said offline apparatus comprises:

means for an offline apparatus for sending a list, that is, sending said provision prohibition list to said offline apparatus as required on connecting the offline apparatus;

means for an offline apparatus for receiving, that is, receiving said provision prohibition list sent from said online apparatus, and also directly receiving said contents data sent from said information

sending apparatus, or receiving said contents data sent from said information sending apparatus via other online apparatus and offline apparatus; and

means for an offline apparatus for stopping capture of said contents data as required based on said provision prohibition list.

359. The information provision system according to claim 358, wherein:

said online apparatus comprises means for an online apparatus for, if said means for an online apparatus for receiving receives said contents data sent from said offline apparatus, determining whether or not said contents data is provision-prohibited as above and also determining whether or not said information sending apparatus that is the source of the contents data is utilization-prohibited as above based on said provision prohibition list;

said means for an online apparatus for stopping capture stops capture of said contents data in the case where said contents data is provision-prohibited as above and in the case where said information sending apparatus is utilization-prohibited as above according to results of determination acquired from said means for an online apparatus for determining; and

said means for an online apparatus for sending a list sends said provision prohibition list to said offline apparatus in the case where said contents data is provision-prohibited as above and in the case where said information sending apparatus is utilization-prohibited as above.

360. The information provision system according to claim 359, wherein:

said offline apparatus comprises means for an offline apparatus for, if means for an offline apparatus for receiving receives said contents data sent from another offline apparatus, determining whether or not said contents data is provision-prohibited as above and also determining whether or not said information sending apparatus that is the source of the contents data is utilization-prohibited as above based on said provision prohibition list;

means for an offline apparatus for stopping capture stops capture of said contents data in the case where said contents data is provision-prohibited as above and in the case where said information sending apparatus is utilization-prohibited as above according to results of determination acquired from said means for an offline apparatus for determining; and

said means for an offline apparatus for sending a list sends said provision prohibition list to another offline apparatus as above in the case where said contents data is provision-prohibited as above and in the case where said information sending apparatus is utilization-prohibited as above.

361. A list sending apparatus for sending a predetermined list to an information receiving apparatus receiving predetermined contents data sent from an information sending apparatus, comprising:

means for creating a provision prohibition list showing said contents data designated as provision-prohibited; and

means for sending said provision prohibition list to said information receiving apparatus.

362. The list sending apparatus according to claim 361, wherein said means for creating a list registers said information sending apparatus designated as utilization-prohibited on said provision prohibition list.

363. The list sending apparatus according to claim 362, wherein:

said means for creating a list updates said provision prohibition list every time said contents data is designated as provision-prohibited as above or every time said information sending apparatus is designated as utilization-prohibited as above; and

said means for sending sends said provision prohibition list to said information receiving apparatus every time it is updated.

364. An information receiving apparatus for receiving predetermined contents data sent from an information sending apparatus and a predetermined list sent from a list sending apparatus, comprising:

means for receiving a provision prohibition list showing said contents data designated as provision-prohibited sent from said list sending apparatus;

means for holding said provision prohibition list;

means for determining whether or not said contents data sent from said information sending apparatus is provision-prohibited based on said provision prohibition list; and

means for stopping capture of said contents data in the case where the contents data is provision-prohibited as above according to results of determination acquired from said means for determining.

365. The information receiving apparatus according to claim 364, wherein:

said means for holding a list holds said provision prohibition list showing said information sending apparatus designated as utilization-prohibited together with said contents data designated as provision-prohibited as above sent from said list sending apparatus;

said means for determining determines whether or not said contents data sent from said information sending apparatus is provision-prohibited as above and also determines whether or not said information sending apparatus is utilization-prohibited as above based on said provision prohibition list;

said means for stopping capture stops capture of said contents data in the case where said contents data is provision-prohibited as above and in the case where said information sending apparatus is utilization-prohibited as above respectively.

366. The information receiving apparatus according to claim 365, comprising:

one or more online apparatuses connected online to said list sending apparatus and receiving said provision prohibition list; and

one or more offline apparatuses not connected online to said list sending apparatus; and wherein

said online apparatus comprises:

means for an online apparatus for sending a list, that is, sending said provision prohibition list to said offline apparatus on connecting the offline apparatus;

means for an online apparatus for receiving, that is, directly receiving said contents data sent from said information sending apparatus, or receiving said contents data sent from said information sending apparatus via other online apparatus and offline apparatus; and

means for an online apparatus for stopping capture of said contents data as required based on said provision prohibition list; and

said offline apparatus comprises:

means for an offline apparatus for sending a list, that is, sending said provision prohibition list to said offline apparatus as required on connecting the offline apparatus;

means for an offline apparatus for receiving, that is, receiving said provision prohibition list sent from said online apparatus, and also directly receiving said contents data sent from said information sending apparatus, or receiving said contents data sent from said

information sending apparatus via other online apparatus and offline apparatus; and

means for an offline apparatus for stopping capture of said contents data as required based on said provision prohibition list.

367. The information receiving apparatus according to claim 366, wherein:

said online apparatus comprises means for an online apparatus for, if said means for an online apparatus for receiving receives said contents data sent from said offline apparatus, determining whether or not said contents data is provision-prohibited as above and also determining whether or not said information sending apparatus that is the source of the contents data is utilization-prohibited as above based on said provision prohibition list;

said means for an online apparatus for stopping capture stops capture of said contents data in the case where said contents data is provision-prohibited as above and in the case where said information sending apparatus is utilization-prohibited as above according to results of determination acquired from said means for an online apparatus for determining; and

said means for an online apparatus for sending a list sends said provision prohibition list to said offline apparatus in the case where said contents data is provision-prohibited as above and in the case where said information sending apparatus is utilization-prohibited as above.

368. The information receiving apparatus according to claim 367, wherein:

said offline apparatus comprises means for an offline apparatus for, if means for an offline apparatus for receiving receives said contents data sent from another offline apparatus, determining whether or not said contents data is provision-prohibited as above and also determining whether or not said information sending apparatus that is the source of the contents data is utilization-prohibited as above based on said provision prohibition list;

means for an offline apparatus for stopping capture stops capture of said contents data in the case where said contents data is provision-prohibited as above and in the case where said information sending apparatus is utilization-prohibited as above according to results of determination acquired from said means for an offline apparatus for determining; and

said means for an offline apparatus for sending a list sends said provision prohibition list to another offline apparatus as above in the case where said contents data is provision-prohibited as above and in the case where said information sending apparatus is utilization-prohibited as above.

369. An information provision method, comprising:

a sending step of creating a provision prohibition list showing said contents data designated as provision-prohibited and sending the

created provision prohibition list by a list sending apparatus, and also sending predetermined contents data by an information sending apparatus;

a receiving step of receiving said provision prohibition list and also receiving said contents data by an information receiving apparatus;

a determining step of determining whether or not said contents data sent from said information sending apparatus is provision-prohibited as above based on said provision prohibition list by said information receiving apparatus; and

a capture stopping step of stopping capture of said contents data in the case where said contents data is provision-prohibited as above according to results of determination acquired by said determining step.

370. The information provision method according to claim 369, wherein:

said sending step registers said information sending apparatus designated as utilization-prohibited as above on said provision prohibition list and sends it by said list sending apparatus;

said determining step determines by said information receiving apparatus whether or not said contents data is provision-prohibited as above and also determines whether or not said information sending apparatus is utilization-prohibited as above based on said provision prohibition list; and

said capture stopping step stops capture of said contents data in the case where it is determined by said information receiving apparatus that said contents data is provision-prohibited as above and in the case where it is determined by said information receiving apparatus that said information sending apparatus is utilization-prohibited as above respectively.

371. The information provision method according to claim 370, comprising:

an inter-apparatus list sending step of, on connecting said online apparatus to said offline apparatus, sending said provision prohibition list to the offline apparatus between one or more online apparatuses connected online to said list sending apparatus and receiving said provision prohibition list and one or more offline apparatuses not connected online to said list sending apparatus constituting said information receiving apparatus; and

an apparatus capture stopping step of said online apparatus and offline apparatus directly receiving said contents data sent from said information sending apparatus or receiving said contents data sent from said information sending apparatus via other online apparatus and offline apparatus and stopping capture of the contents data as required based on said provision prohibition list.

372. The information provision method according to claim 371, comprising:

a first determination step of, if said contents data is sent from said offline apparatus, said online apparatus determining whether or not said contents data is provision-prohibited as above and also determining whether or not said information sending apparatus that is the source of the contents data is utilization-prohibited as above based on said provision prohibition list; and

a first inter-apparatus list sending step of stopping capture of said contents data and also sending said provision prohibition list to said offline apparatus in the case where said contents data is provision-prohibited as above and in the case where said information sending apparatus is utilization-prohibited as above respectively.

373. The information provision method according to claim 372, comprising:

a second determination step of, if said contents data is sent from another offline apparatus, said offline apparatus determining whether or not said contents data is provision-prohibited as above and also determines whether or not said information sending apparatus that is the source of the contents data is utilization-prohibited as above based on said provision prohibition list; and

a second inter-apparatus list sending step of stopping capture of said contents data and also sending said provision prohibition list to another offline apparatus as above in the case where said contents data is provision-prohibited as above and in the case where said

information sending apparatus is utilization-prohibited as above respectively.

374. A list sending method for sending a predetermined list to an information receiving apparatus receiving predetermined contents data sent from an information sending apparatus, comprising:

a list creating step of creating a provision prohibition list showing said contents data designated as provision-prohibited; and

a sending step of sending said provision prohibition list to said information receiving apparatus.

375. The list sending method according to claim 374, wherein said list creating step registers said information sending apparatus designated as utilization-prohibited on said provision prohibition list.

376. The list sending method according to claim 375, wherein:

said list creating step updates said provision prohibition list every time said contents data is designated as provision-prohibited as above or every time said information sending apparatus is designated as utilization-prohibited as above; and

said sending step sends said provision prohibition list to said information receiving apparatus every time it is updated.

377. An information receiving method for receiving predetermined contents data sent from an information sending apparatus and a predetermined list sent from a list sending apparatus, comprising:

a receiving step of receiving a provision prohibition list showing said contents data designated as provision-prohibited sent from said list sending apparatus;

a determining step of determining whether or not said contents data sent from said information sending apparatus is provision-prohibited based on said provision prohibition list; and

a capture stopping step of stopping capture of said contents data in the case where the contents data is provision-prohibited as above according to results of determination acquired from said determining step.

378. The information receiving method according to claim 377, wherein:

said receiving step receives said provision prohibition list showing said information sending apparatus designated as utilization-prohibited together with said contents data designated as provision-prohibited as above sent from said list sending apparatus;

said determining step determines whether or not said contents data sent from said information sending apparatus is provision-prohibited as above and also determines whether or not said information sending apparatus is utilization-prohibited as above based on said provision prohibition list;

said capture stopping step stops capture of said contents data in the case where said contents data is provision-prohibited as above and in the case where said information sending apparatus is utilization-prohibited as above respectively.

379. An information receiving method by an online apparatus connected online to said list sending apparatus, comprising:

an online apparatus receiving step of receiving said provision prohibition list sent from said list sending apparatus, and also directly receiving said contents data sent from said information sending apparatus, or receiving said contents data sent from said information sending apparatus via another online apparatus as above or an offline apparatus not connected online to said list sending apparatus; and

an online apparatus sending step of sending said provision prohibition list to said offline apparatus on connecting the offline apparatus.

380. The information receiving method according to claim 379, comprising:

an online apparatus determining step of determining whether or not said contents data is provision-prohibited as above and also determining whether or not said information sending apparatus is utilization-prohibited as above based on said provision prohibition list;

an online apparatus capture stopping step of stopping capture of said contents data in the case where said contents data is provision-prohibited as above and in the case where said information sending apparatus is utilization-prohibited as above respectively.

381. The information receiving method according to claim 380, wherein:

said online apparatus sending step sends said provision prohibition list to said offline apparatus when receiving said contents data sent from said offline apparatus in the case where said contents data is provision-prohibited as above and in the case where said information sending apparatus is utilization-prohibited as above.

382. An information receiving method by an offline apparatus not connected online to a list sending apparatus, comprising:

an offline apparatus receiving step of, on connecting an online apparatus connected online to said list sending apparatus, receiving said provision prohibition list sent from the online apparatus, and also directly receiving said contents data sent from said information sending apparatus, or receiving said contents data sent from said information sending apparatus via another online apparatus or offline apparatus as above; and

an offline apparatus sending step of, on connecting another offline apparatus as above, sending said provision prohibition list as required to the offline apparatus.

383. The information receiving method according to claim 382, comprising:

an offline apparatus determining step of determining whether said contents data is provision-prohibited as above and also determining whether or not said information sending apparatus is utilization-prohibited as above based on said provision prohibition list;

an offline apparatus capture stopping step of stopping capture of said contents data in the case where said contents data is provision-prohibited as above and in the case where said information sending apparatus is utilization-prohibited as above respectively.

384. The information receiving method according to claim 383, wherein:

said offline apparatus sending step sends said provision prohibition list to another offline apparatus as above when receiving said contents data sent from another offline apparatus as above in the case where said contents data is provision-prohibited as above and in the case where said information sending apparatus is utilization-prohibited as above.

385. A program storage medium storing a predetermined program and supplying the program to a list sending apparatus, characterized in that said program comprises:

a list creating step of creating a provision prohibition list showing predetermined contents data designated as provision-prohibited; and

a sending step of sending said provision prohibition list to an information receiving apparatus receiving said contents data.

386. The program storage medium according to claim 385, wherein:

said list creating step of said program registers said information sending apparatus designated as utilization-prohibited on said provision prohibition list, of information sending apparatuses sending said contents data to said information receiving apparatus.

387. The program storage medium according to claim 386, wherein:

said list creating step of said program updates said provision prohibition list every time said contents data is designated as provision-prohibited as above or every time said information sending apparatus is designated as utilization-prohibited as above; and

said sending step sends said provision prohibition list to said information receiving apparatus every time it is updated.

388. A program storage medium storing a predetermined program and supplying the program to an information receiving apparatus, characterized in that said program comprises:

a receiving step of receiving a provision prohibition list showing predetermined contents data designated as provision-prohibited sent from a list sending apparatus;

a determining step of determining whether or not said contents data sent from an information sending apparatus is provision-prohibited as above based on said provision prohibition list; and

a capture stopping step of stopping capture of said contents data in the case where the contents data is provision-prohibited as above according to results of determination acquired from said determining step.

389. The program storage medium according to claim 388, wherein:

said receiving step of said program receives said provision prohibition list showing said information sending apparatus designated as utilization-prohibited together with said contents data designated as provision-prohibited as above sent from said list sending apparatus;

said determining step determines whether or not said contents data sent from said information sending apparatus is provision-prohibited as above and also determines whether or not said information sending apparatus is utilization-prohibited as above based on said provision prohibition list;

said capture stopping step stops capture of said contents data in the case where said contents data is provision-prohibited as above and in the case where said information sending apparatus is utilization-prohibited as above respectively.

390. A program storage medium storing a predetermined program and supplying the program to an online apparatus, characterized in that said program comprises:

an online apparatus receiving step of receiving said provision prohibition list sent from said list sending apparatus, and also directly receiving said contents data sent from said information sending apparatus, or receiving said contents data sent from said information sending apparatus via another online apparatus connected online to the list sending apparatus or an offline apparatus not connected online to said list sending apparatus; and

an online apparatus sending step of sending said provision prohibition list to said offline apparatus on connecting the offline apparatus.

391. The program storage medium according to claim 390, wherein said program comprises:

an online apparatus determining step of determining whether or not said contents data is provision-prohibited as above and also determining whether or not said information sending apparatus is utilization-prohibited as above based on said provision prohibition list;

an online apparatus capture stopping step of stopping capture of said contents data in the case where said contents data is provision-prohibited as above and in the case where said information sending apparatus is utilization-prohibited as above respectively.

392. The program storage medium according to claim 391, wherein:

said online apparatus sending step of said program sends said provision prohibition list to said offline apparatus when receiving said contents data sent from said offline apparatus in the case where said contents data is provision-prohibited as above and in the case where said information sending apparatus is utilization-prohibited as above.

393. A program storage medium storing a predetermined program and supplying the program to an offline apparatus, characterized in that said program comprises:

an offline apparatus receiving step of, on connecting an online apparatus connected online to a list sending apparatus, receiving said provision prohibition list sent from the online apparatus, and also directly receiving said contents data sent from said information sending apparatus, or receiving said contents data sent from said information sending apparatus via another online apparatus as above or an offline apparatus not connected online to said list sending apparatus; and

an offline apparatus sending step of sending said provision prohibition list as required to another offline apparatus as above on connecting the offline apparatus.

394. The program storage medium according to claim 393, wherein said program comprises:

an offline apparatus determining step of determining whether or not said contents data is provision-prohibited as above and also determining whether or not said information sending apparatus is utilization-prohibited as above based on said provision prohibition list;

an offline apparatus capture stopping step of stopping capture of said contents data in the case where said contents data is provision-prohibited as above and in the case where said information sending apparatus is utilization-prohibited as above respectively.

395. The program storage medium according to claim 394, wherein:

said offline sending step of said program sends said provision prohibition list to another offline apparatus as above when receiving said contents data sent from another offline apparatus as above in the case where said contents data is provision-prohibited as above and in the case where said information sending apparatus is utilization-prohibited as above.